Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

CYBER INCIDENT RESPONSE PLAN

REDBACK OPERATIONS

cyber.gov.au

Table of Contents

1. Authority and Review

Document Control and Review

Document Control	
Author	**Indiah Smith**
Owner	**Indiah Smith**
Date created	**14 November 2023**
Last reviewed by	**Indiah Smith**
Last date reviewed	**2 December 2023**
Endorsed by and date	**Ben Stephens on 2 December 2023**
Next review due date	**2 December 2024**

Version Control

Version	Date of Approval	Approved By	Description of Change
0.1	2 December 2023	Action Officer	Initial Draft

2. Purpose and Objectives

Purpose of the CIRP

The Cyber Incident Response Plan (CIRP) is a piece of documentation recommended by the Australian Cyber Security Centre (ACSC). It serves the purpose of assisting organisations in developing a plan and checklist to efficiently manage cyber incidents and enforce appropriate recovery and response mechanisms. The CIRP will assist personnel in fulfilling their roles in adherence to legal and regulatory responsibilities. Effective use of the CIRP will mitigate threats and build consumer trust in the company. Regular testing and review will ensure the plan is up-to-date with emerging threats and developments.

Objectives of the CIRP

1. To identify the incident response and responsibilities and roles of key stakeholders;
2. To assist employees with identifying workplace risks, types of incidents and severity levels;
3. To describe annual testing requirements and post-incident procedures;
4. To comply with government-mandated protocols and regulatory obligations; and
5. To identify areas for improvement in the post-incident stages.

3. Standards and Frameworks

State/territory government standards and framework

- Victoria's Cyber Security Strategy 2021
- Australia's Cyber Security Strategy 2020

National standards and frameworks

- Australian Government Information Security Manual
- Australian Prudential Regulation Authority (APRA) Prudential Practice Guide CPG 234 Information Security

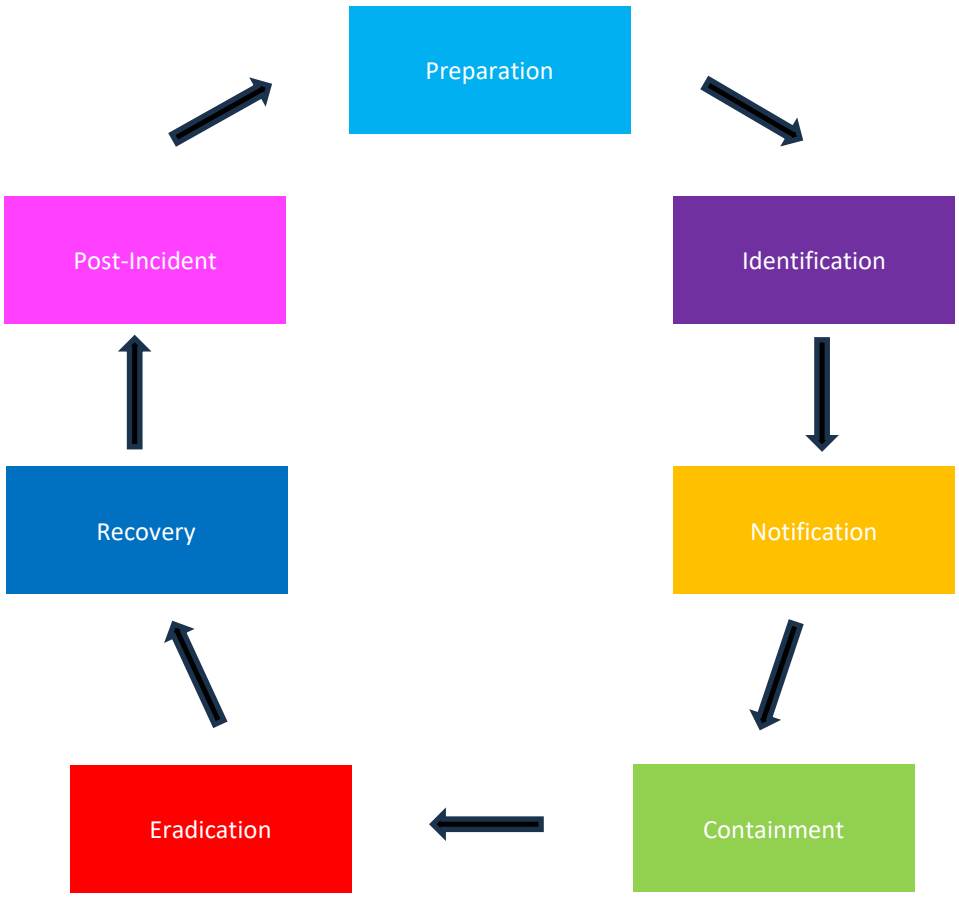
Industry standards and frameworks

- Australian Information Security Guide for Small Healthcare Businesses

International standards and frameworks

- NIST Computer Security Incident Handling Guide
- International Standard ISO/IEC 27035-2:2016
- International Standard ISO/IEC 27035-3:2020
- International Standard ISO/IEC 27035-1:2023

4. High Level Incident Response Process



5. Common Security Incidents and Responses

A list of commonly used terms and definitions is provided at Appendix A.

5.1. Common Threat Vectors

The following table contains common threat vectors from the NIST Computer Security Incident Handling Guide.

Type	Description
External/Removable Media	An attack executed from removable media or a peripheral device (e.g. malicious code spreading onto a system from an infected USB flash drive).
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g. a DDoS intended to impair or deny access to a service or application or a brute force attack against an authentication mechanism, such as passwords).
Web	An attack executed from a website or web-based application (e.g. a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware).
Email	An attack executed via an email message or attachment (e.g. exploit code disguised as an attached document or a link to a malicious website in the body of an email).
Supply Chain Interdiction	An antagonistic attack on hardware or software assets utilising physical implants, Trojans or backdoors, by intercepting and modifying an asset in transit from the vendor or retailer.
Impersonation	An attack involving replacement of something benign with something malicious (e.g. spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation).
Improper usage	Any incident resulting from violation of an organisation's acceptable usage policies by an authorised user, excluding the above categories (e.g. a user installs file sharing software, leading to the loss of sensitive data).
Loss or Theft of Equipment	The loss or theft of a computing device or media used by an organisation (e.g. a laptop, smartphone or authentication token).

5.2. Common Cyber Incidents

The following table provides a list of common cyber incident types and corresponding initial response activities.

Type/Description	Response
Denial of Service (DoS) and Distributed Denial of Service (DDoS): overwhelming a service with traffic, sometimes impacting availability.	A network pipe saturation will trigger an alert to a member allocated to the tier 1 Network Operation Centre team. The team member should notify the security manager responsible for mitigation procedures. The security manager should determine that the DDoS attack is occurring prior to escalating the issue and consulting the DDoS mitigation playbook.
Phishing: deceptive messaging designed to elicit users' sensitive information (such as banking logins or business login credentials) or used to execute malicious code to enable remote access.	A team member should report the cyber incident to the Service Desk and refer to the data breach playbook. The cyber incident should be classified and reported to the Information Security Manager and all affected data or systems should be identified.
Ransomware: a tool used to lock or encrypt victims' files until a ransom is paid.	Once ransomware is detected, the risks to the organisation should be assessed and a threat analysis should be undertaken to identify vulnerabilities. Further, the scope of the attack should be defined to determine the amount of data and systems that have been impacted. These systems should be isolated and disabled to prevent further spread.
Malware: a Trojan, virus, worm, or any other malicious software that can harm a computer system or network.	A team member should report the malware once detected. This should be escalated to the cyber security manager who should investigate log files and determine the initial date and point of infection. All infected systems should be isolated and infected accounts should be disabled.
Data breach: unauthorised access and disclosure of information.	A team member should contact the cyber security manager upon detection of the breach. The cyber security manager should assess the risk and make a record. This should be escalated to the Director of the company who should consider making a breach notification.
Industrial Control System compromise: unauthorised access to ICS.	Personnel should engage into scanning operating systems to detect unauthorised access. This should be reported to the cyber security manager who should coordinate actions to contain or eradicate the threat.

6. Roles and Responsibilities

This section includes details of the roles and responsibilities of core individuals and teams responsible for incident response and decision making, including the operational level Cyber Incident Response Team (CIRT) and the strategic level Senior Executive Management Team (SEMT).

All personnel listed here should be familiar with their responsibilities in this plan and practise their response.

See Appendix L for details of current personnel in the below roles.

6.1. Points of Contact for Reporting Cyber Incidents

Primary and secondary (backup) internal points of contact to report cyber incidents to over a 24/7 period.

Role Title	Hours of Operation	Responsibilities
Cyber Security Policy Advisor	9:00am – 5:30pm	Creating, reviewing and assessing policies and procedures and overseeing risk management.

6.2. Cyber Incident Response Team (CIRT)

CIRT members responsible for managing responses to cyber incidents:

Organisation Role	Hours of Operation	CIRT Role Title	CIRT Responsibilities
Cyber Security Team Leader	9:00am-5:30pm	Team Leader	Coordinates activities of the incident response team, and the focus of the team in minimising damage and facilitating recovery
Senior Cyber Security Team Member	9:00am-5:30pm	Lead Investigator	Collects and analyses evidence for the purpose of determining the issue and implementing appropriate recovery mechanisms
Senior Cyber Security Team Member	9:00am-5:30pm	Communications Lead	Coordinates communication efforts with internal and external stakeholders
Senior Cyber Security Team Member	9:00am-5:30pm	Documentation and Timeline Lead	Logging team activities and engaging in record keeping of investigation and recovery tasks on an incident timeline
Junior Cyber Security Team Member	9:00am-5:30pm	HR Representative	Responsible for providing support to employees and the communication is effective and compliant with company policy

For more significant cyber security incidents the CIRT could be expanded to include:

Organisation Role	Hours of Operation	CIRT Role Title	CIRT Responsibilities
Company Leader	9:00am – 5:30pm	Company Leader	Responsible for ensuring the incident is communicated, documented or escalated effectively
Company Acting Director	9:00am – 5:30pm	Company Director	Responsible for supporting critical decision-making

6.3. Senior Executive Management Team (SEMT)

Significant cyber incidents may require the formation of the SEMT to provide strategic oversight, direction and support to the CIRT, with a focus on:

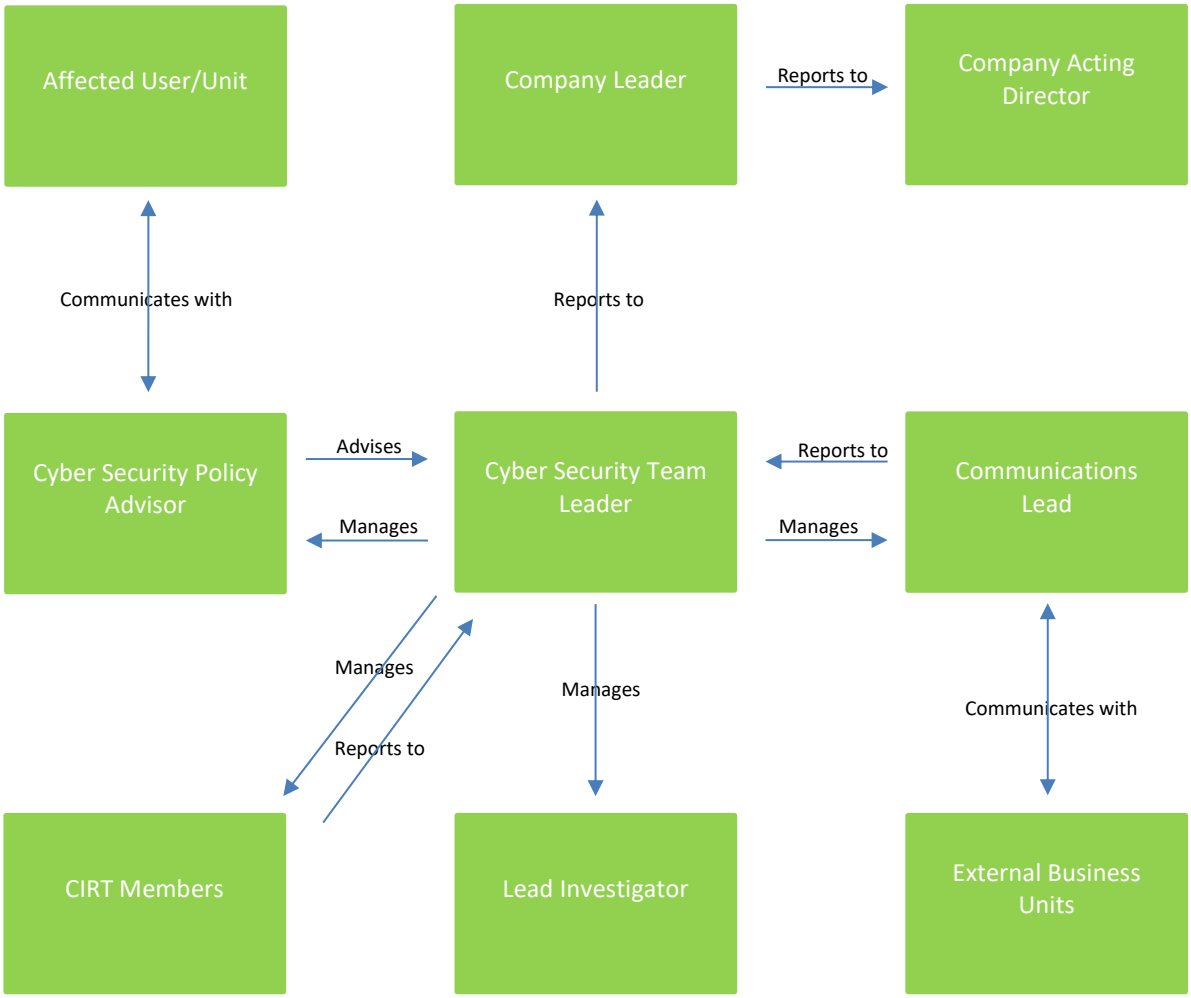
- Strategic issues identification and management
- Stakeholder engagement and communications (including Board and ministerial liaison, if applicable)
- Resource and capability demand (including urgent logistics or finance requirements, and human resources considerations during response effort).

SEMT members responsible for managing responses to cyber incidents:

Hours of Operation	Hours of Operation	SEMT Role
Company Leader	9:00am – 5:30pm	Responsible for ensuring the incident is communicated, documented or escalated effectively
Company Acting Director	9:00am – 5:30pm	Responsible for supporting critical decision-making

6.4. Roles and Relationships

The following diagram reflects the relationship between the key personnel and teams involved in the response.



7. Communications

Communications are an integral part of incident management and essential in responding to and recovering from cybersecurity incidents. Stakeholders should be informed on how they are affected and the appropriate steps to take, with careful consideration of ensuring information is not provided to the attacker to exacerbate the incident.

Following the assessment of the situation and the information-gathering process, communication must be actioned as soon as possible by the Communications Lead who will sign-off messages to the internal and external stakeholders.

The company will support communications between the CIRT and SEMT and facilitate effective internal and external communications.

The incident response team process will be activated upon reports to the customer or IT Helpdesk who will support employees and consumers suspecting a security incident.

The communication should be focused on building trust with stakeholders and expressing commitment to controlling the situation and acknowledging the risks involved.

7.1. Internal Communications

Internal Stakeholders

Internal stakeholders include the following parties.

1. Employees;
2. Managers;
3. Partners; and
4. Regulatory bodies

Notification Procedures

In the event of a cyber incident, incident stakeholders should be notified following an assessment of the incident and appropriate action-taking steps should be clearly communicated.

The Communications Lead will be responsible for gathering information and clearly setting out the process within a reasonable time following the discovery of the incident.

In the initial briefing, the incident response team should determine the type of incident, who is affected, how widespread the incident is, any immediate impacts and whether the risk may increase.

The HR Representative involved in the CIRT should oversee these efforts and provide active support to internal stakeholders to ensure proper reporting requirements are fulfilled. Furthermore, they should review the communications to establish the right tone, communication frequency and format for each internal audience.

7.2. External Communications

External Stakeholders

External stakeholders include the following parties.

1. Customers;
2. General public;
3. Creditors;
4. Suppliers; and

5. Government

Notification Procedures

A cyber incident response communication channel should be implemented to ensure stakeholders are provided with regular updates and reassured that an investigation is ongoing.

The situation should be assessed to determine the most appropriate communication channel and whether the company should use written correspondence via post, email, phone, social media or the website. Alternative contact methods such as a phone number, online chat system and email should be provided to external stakeholders to get in contact with the company such as a phone number.

If a publication or documentation is deemed appropriate by company leads, it must comprise a purpose, basic structure, distribution method and an identification mechanism.

The message should avoid technical terminology and it should be clearly stated that steps are being undertaken to minimise the threat and protect sensitive data. It should explain what the company is doing to deal with the incident and the expected outcome of these actions.

Regular updates should be communicated and the company should maintain a transparent line of communication to reinforce trust in the community. This should be supported by empathy and positivity that the company will engage in efforts to overcome the crisis.

All communications should state that the information is confidential and should not be disclosed to protect the company against potential regulatory proceedings and reputational damage.

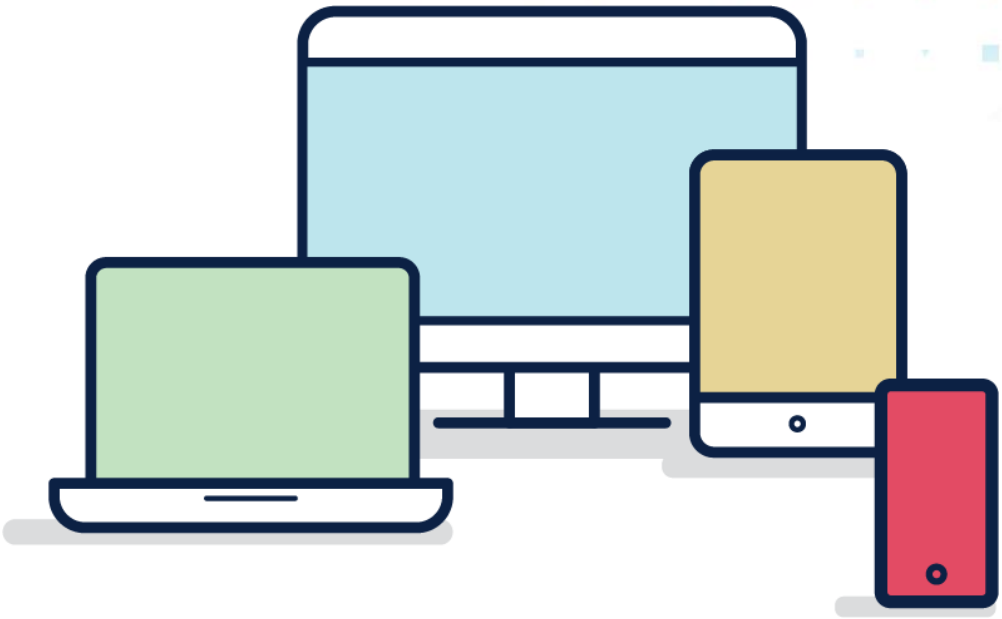
Legal representatives of the company should advise regulators on how the company is complying with the relevant laws and standards.

Reporting Requirements

After identification of a critical cyber security incident, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) should be notified within 12 hours if the incident is deemed to have had a significant impact on the availability of the essential goods and services provided by the company.

If the incident has had or has the potential to have an impact on an asset of the business, the ASD's ACS must be notified within 72 hours of recognising the incident.

Reporting requirements are mandated by the *Security of Critical Infrastructure Act 2018* (SOCI Act) and legal personnel should be consulted to oversee compliance with this Act.



8. Supporting Procedures and Playbooks

8.1. Supporting Standard Operating Procedures (SOPs)

The Standard Operating Procedures (SOPs) available to support incident response efforts include:

- NIST Cybersecurity Framework
- NIST 800-171
- ISO 27002
- NIST 800-53 R5

8.2. Supporting Playbooks

Incident response playbooks follow the 7 steps outlined in the NIST incident response procedure:

1. Prepare
2. Detect
3. Analyse
4. Contain
5. Eradicate
6. Recover
7. Post-Incident Handling

The playbooks available to provide step-by-step guidance for responses to common incidents include:

- Malware Outbreak Incident Response Playbook;
- Phishing Incident Response Playbook;
- Data Theft Incident Response Playbook;
- Virus Outbreak Incident Response Playbook;
- Denial of Service Incident Response Playbook;
- Unauthorised Access Incident Response Playbook;
- Elevation of Privilege Incident Response Playbook;
- Root Access Incident Response Playbook;
- Improper Usage Incident Response Playbook; and
- Redback Operations Recovery Playbook.

9. Jurisdictional and National Incident Response Arrangements

The state and/or territory and national arrangements are detailed in this section.

9.1. Jurisdictional Arrangements

13.1.1. Victorian Protective Data Security Standards V2.0

The Standards establish 12 requirements to protect public sector information.

Standard 6 refers to Information Security Incident Management and mandates that an organisation must establish, implement and maintain an information security incident management process.

The elements require:

(a) The organisation document and communicate the processes and plans for information security incident management;

(b) The organisation expressly details the roles and responsibilities required for information security incident management;

(c) The organisation's information security incident management process and plain contain the following phases:

(i) Plan and prepare;

(ii) Detect and report;

(iii) Assess and decide;

(iv) Response (contain, eradicate, recover, notify); and

(v) Lessons learnt.

(d) The organisation records information security incidents in a register;

(e) The organisation's information security incident management procedures identify and categorise administrative incidents in contrast to criminal incidents and investigative handover; and

(f) The organisation regularly tests its incident response plan.

9.2. National Arrangements and Regulatory Requirements

9.2.1. Privacy Act 1988 (Cth)

Redback Operations is required to comply with the provisions of the *Privacy Act 1988* (Cth) 'the Act'. Under Part IIIC of the Act, an entity must provide notification to the OAIC and any affected individuals in the event of a data breach concerning personal information that is likely to cause serious harm.

As a small business operation with under a $3 million annual turnover, compliance under the Act will be required.

1 Notification Requirements

(a) The OAIC must be notified once the business is aware of a data breach.

(b) Any suspected data breaches permit the business 30 days to investigate.

(c) The notification to the OAIC and the affected individuals must contain:

1. The details of the APP entity
2. An explanation of the data breach;
3. The types of information affected; and
4. Suggested procedural steps for individuals to follow in response to the breach.

2 When to notify the OAIC

The OAIC and affected individuals must be notified in the event that:

(a) The business believes on reasonable grounds that a data breach has eventuated; or

(b) The OAIC directs the business to submit a written notification.

3 Notice form

Data breaches must be reported through the online notification portal on the OAIC's website.

The company should use its discretion to notify individuals and do so through a regularly used form of communication. In the event that the impacted individuals cannot be contacted, the company may opt for a public statement made on the website.

4 Elements constituting a data breach

A data breach will have occurred if:

(a) There is unauthorised access to, unauthorised disclosure of, or loss of, personal information stored by an entity and

(b) The access, loss or disclosure has the potential to result in serious harm to any of the individuals to whom the information is related.

5 Personal information

(a) Personal information refers to information about an individual, or an individual who can be reasonably identified:

1. If the information or opinion is accurate or not; and
2. If the information or opinion is recorded in written form or not.

Appendix C provides the ACSC's incident triage questions.

10. Incident Notification and Reporting

Processes for internal and external incident notification and reporting include:

Incident type/ threshold	Organisation/agency to receive notification or report	Contact details for the notifying organisation/agency	Key notifying/reporting requirements and link to organisation/agency information	Personnel responsible
Ransomware	Australian Cyber Security Centre (ACSC)	P: 1300 CYBER1 E: asd.assist@defence.gov.au	Refer to https://www.cyber.gov.au/acsc/report	Indiah Smith
Data breach	Office of the Australian Information Commissioner (OAIC)	See contact details at https://www.oaic.gov.au/about-us/contact-us/	Refer to https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/	Indiah Smith

10.1. Insurance

The company is insured by Chubb as the leading provider of cyber risk solutions under the Cyber Enterprise Risk Management (ERM) Policy which is in place to protect business assets against cyber threats.

Chubb supports the incident response efforts enforced by Redback Operations and provides local and global cyber expertise.

The cyber insurance policy covers the below incidents:

- Any interruption to the activities of the business as a result of network security failures or attacks, human errors, or programming errors;
- Data loss and restoration;
- Incident investigation costs and response;
- Disruption, delay and expenses towards reputation mitigation;
- Communications during crisis reputational mitigation expenses;
- Liability regarding data confidentiality;
- Liability regarding unauthorised network usage;
- Data or network extortion;
- Media liability; and
- Expenses relating to regulatory investigations.

INCIDENT RESPONSE PROCESS

11. Detection, Investigation, Analysis and Activation

11.1. Incident Classification

For example:

Incident Classification	Descriptions
Critical	• Customers unable to access client-facing services • Critical infrastructure systems offline • Loss of customer data • Breach of confidentiality or privacy • Reputational damage that is likely to have long-term impacts • Severe financial impact
High	• A group of customers unable to access client-facing services • Non-critical infrastructure systems offline • Potential loss of customer data • Potential breach of confidentiality or privacy • Moderate reputational damage
Medium	• A handful of customers are unable to access client-facing services • Some non-critical infrastructure systems offline • Potential reputation damage
Low	• Minor inconveniences for customers accessing client-facing services • Temporary disturbance to non-critical systems • Minor performance issues

For information about the ACSC Incident Categorisation Matrix see Appendix K.

11.2. Cyber Incident Response Team (CIRT) Activation

The CIRST should be activated in line with the Incident Classification framework. Any suspicious activity, viruses or attackers should be a trigger for this response. Cyber security specialists can respond quickly and this will in turn reduce damage and overall costs for the business.

11.2.1 Logistics and Communications

This section refers to the logistical and communication protocols that support incident response. The cyber security team are located on Floor 10 of the premises in the Security Operations Centre and have access to the following essential pieces of physical equipment necessary to respond to cyber incidents:

- Analysis laptop with forensic tools and necessary playbooks installed;
- Ethernet cable; and
- Clean hard drives.

Depending on the circumstances of the attack, the following soft tools may be required:

- Networking security monitoring tools;
- Encryption tools;
- Web vulnerability scanning tools;
- Penetration testing tools;
- Antivirus software;
- Network intrusion detection;
- Packet sniffers; and
- Firewall tools.

Communication will be facilitated through Microsoft Teams which provides phone and teleconference capabilities.

11.3. Investigation Questions

To guide the incident response efforts and understanding of the scope and impact of the incident, the below list of investigation questions for each incident should be referred to. Not all questions may be answerable with the data available and questions may change as the investigation progresses.

Possible initial investigation questions include:

- Has data has been compromised by the incident and, if so, what type of data?
- What was the method and pathway used by the attacker to access the system?
- What activity occurred in the post-exploitation phase?
- Have accounts been jeopardised?
- What level of privilege do the threatened accounts have?
- Does the actor have control of the network or device?
- Is the actor suspected to compromise other areas of the organisation and if so, which branches?

11.4. Escalation and De-escalation

The triggers and/or thresholds and decision making authorities for incident escalation and de-escalation include:

Incident Classification	Action	Triggers and/or thresholds for escalation and de-escalation	Minimum level authority
Critical	De-escalate to High	Company acting director recognises that the incident will have a severe effect on the operations of the business with lasting long-term effects	Company acting director
High	Escalate to Critical	Cyber security leader recognises that the incident will have an impact on the operations of the business	Company leader

	De-escalate to Medium	Cyber security leader recognises that the incident will have a minimal effect on the operations of the business	Cyber security leader
Medium	Escalate to High	Cyber security leader recognises that the incident may pose a risk to some operations of the business	Cyber security leader
	De-escalate to Low	Cyber security team member deems that the risk can be controlled and will not pose a serious risk to the operations of the business	Cyber security team member
Low	Escalate to Medium	Company employee determines the incident may impact the operations of the business	Company employee

12. Containment, Evidence Collection & Remediation

12.1. Containment

The Cyber Security Team Leader is responsible for containment and will document the containment activities occurring in an incident.

Containment is the process of a strategy during a security event that is responsible for minimising the security incident and preventing the spread or escalation of the incident. This requires looking at evidence collected during the detection and analysis of the incident such as identifying impacted hosts, attackers, malware, and monitoring of attacking communication channels. It is essential that containment strategies are executed simultaneously to prevent attackers from escalating the attack.

The organisation should consult the NIST SP 800-61 Computer Security Incident Handling Guide.

The below criteria should be considered to determine the strategy of containment.

- Possible resource theft or damage to assets;
- The requirement to preserve evidence;
- Any additional impacts there could be to systems/services
- Time and resources required to contain the incident
- Effectiveness of the containment solution (e.g. partial vs full containment)
- Duration that the solution will remain in place (e.g. temporary vs permanent solution)

12.2. Documentation

The Cyber Security team lead is responsible for documenting all cyber incidents. This should include the initial responder to the incident, what was impacted, how the incident occurred, the actions taken and how the actions assisted. Should the situation be escalated, this will assist the process of gathering evidence and assist the response team in dealing with future incidents of the same nature. Documentation should cover the declaration, remediation and recovery of the incident.

Refer to Appendix D for a Situation Report template and Appendix E for an Incident Log template.

Situation reports should contain the following information:

- Time and date of the incident
- Incident status
- Classification and type of the incident
- Impact and breadth of the incident
- Severity
- Necessary external assistance and resources
- Incident resolution actions and procedures
- Incident manager contact details and key CIRT personnel

12.3. Evidence Collection and Preservation

When gathering evidence, maintain a detailed log that clearly documents how all evidence has been collected. This should include who collected or handled the evidence, the time and date (including time zone) evidence was collected and handled, and the details of each item collected (including the physical location, serial number, model number, hostname, media access control (MAC) address, IP address and hash values). See the Evidence Register template at Appendix F to capture this information.

12.4. Remediation Action Plan

The Remediation Action Plan determines the incident containment process and eradication of the threat. It also establishes the evidence collection process and takes place following repair of the systems and after instructions have been provided to affected parties. An analysis must confirm remediation of the incident. See Appendix G for a template.

In the process of establishing the Remediation Action Plan, consideration should be given to the following:

- What steps should be taken to resolve the incident?
- Who is responsible for conducting the remediation efforts?
- What systems and services should be prioritised?
- What additional resources are necessary to resolve the incident?
- What systems and services will be impacted during the remediation process?
- What is the anticipated resolution timeframe?

13. Recovery

After containment and eradication, the recovery plan focuses on efficiently restoring IT systems to ensure business can proceed as usual and prevent further loss from occurring. The recovery plan provides guidance for managing the cybersecurity incident. Reference should be made to the NIST Special Publication 800-184 Guide to Cybersecurity Event Recovery and the Redback Operations Recovery Playbook. Recovery is comprised of two phases including combatting the incident and mitigating future incidents.

The objective of the recovery plan is as follows:

- Business continuity;
- Communicating with stakeholders
- Compliance with legal and regulatory requirements and deadlines;
- Safeguarding confidential and sensitive data;
- Reducing loss and subsequent costs;
- Restoring operations; and
- Implementing improvements.

The recovery efforts will be led by the Cyber Security Policy Advisor, in conjunction with the cyber security team. The team should convene immediately to determine the methods of restoring systems to normal operations and the timeframes should be estimated.

After the response lead completes Appendix D, the cyber security team should perform an incident analysis to determine the key functions impacted by the incident.

A monitoring strategy should be implemented after the assessment of the incident to ensure the systems are functioning appropriately.

Legal obligations should be assessed and reporting requirements should be adhered to and the communication strategy should be adhered to in order to keep stakeholders informed.

Following the execution of the response, an evaluation of the effectiveness of the response should be undertaken to prevent similar incidents. During the recovery process, the weaknesses of the business should be identified and long-term objectives should be implemented for the purpose of continuous improvement. This may include flaws in technologies, people and processes.

The organisation should undergo frequent cyber security testing and analyse the results to test its cyber security capabilities and effectively manage risks. This will improve the competency of employees and strengthen the pre-existing plan.

A formal debrief should be implemented at the end of the CIRT operations to discuss improvements to the response procedure.

13.1. Stand Down

All operations of the CIRT should continue until the Cyber Security Team Leader formally stands down the CIRT. The SEMT also has authority to execute this decision-making.

Stand down may occur at any point of time provided the recovery phase is under control and normal business operations can proceed. This can be actioned at the commencement of the recovery phase, during the recovery phase or at the end of the recovery phase.

13.1.1 Incident Reporting Process

The Cyber Security Team Leader is responsible for coordinating the efforts of the CIRT in completing an incident report. The reporting timeframes in 7.2 should be adhered to. Upon closing the report, the SEMT team should provide feedback on the incident and sign off on the report. This report should be stored on the company database for future reference and to hold the organisation accountable for carrying out the next steps.

The report should include the information in Appendix D:

a) Date and Time incident detected;
b) Current Status;
c) Incident Type;
d) Incident Classification;
e) Scope;
f) Impact;
g) Severity;
h) Notifications Actioned/Pending;
i) Assistance required;
j) Actions taken to resolve incident;
k) Contact details for incident manager; and
l) Date and Time of next update.

The additional sections below may also be referred to in an detailed in-depth report.

a) Date and time of the incident;
b) Name and contact details of the company;
c) Details of the company's size, name and industry;
d) The attack vector or vulnerability;
e) Details of the discovery of the cybersecurity incident;
f) The impacted assets;
g) Operational disruptions to the company;

14. Learn and Improve

14.1. Post Incident Review

A Post Incident Review (PIR) is a detailed process of analysis following a cyber security incident to prevent future incidents. Learning material obtained through this process will be incorporated into the CIRP to strengthen the incident handling capability.

Key factors to be considered in the PIR:

- What was the cause of the incident?
- Did the incident response team encounter any issues?
- Could the incident have been prevented and if so, what steps should have been taken?
- What strategies were effective in responding to the incident?
- What improvements can be made to response to future incidents?

The PIR Guide and Template with more detailed questions to consider is available at Appendix H. Recommendations that arise from the review can be documented in a corresponding Action Register. Use the template at Appendix I.

14.1.1 PPOSTTE Model

The PPOSTTE model can assist to reflect on key elements of the incident response.

People	Roles, responsibilities, accountabilities, skills
Process	Plans, policies, procedures, protocols, processes, templates, arrangements
Organisation	Structures, culture, jurisdictional arrangements
Support	Infrastructure, facilities, maintenance
Technology	Equipment, systems, standards, security, inter-operability
Training	Qualifications/skill levels, identification of required courses
***Exercise Management** *This only applies to exercises*	Exercise development, structure, management, conduct

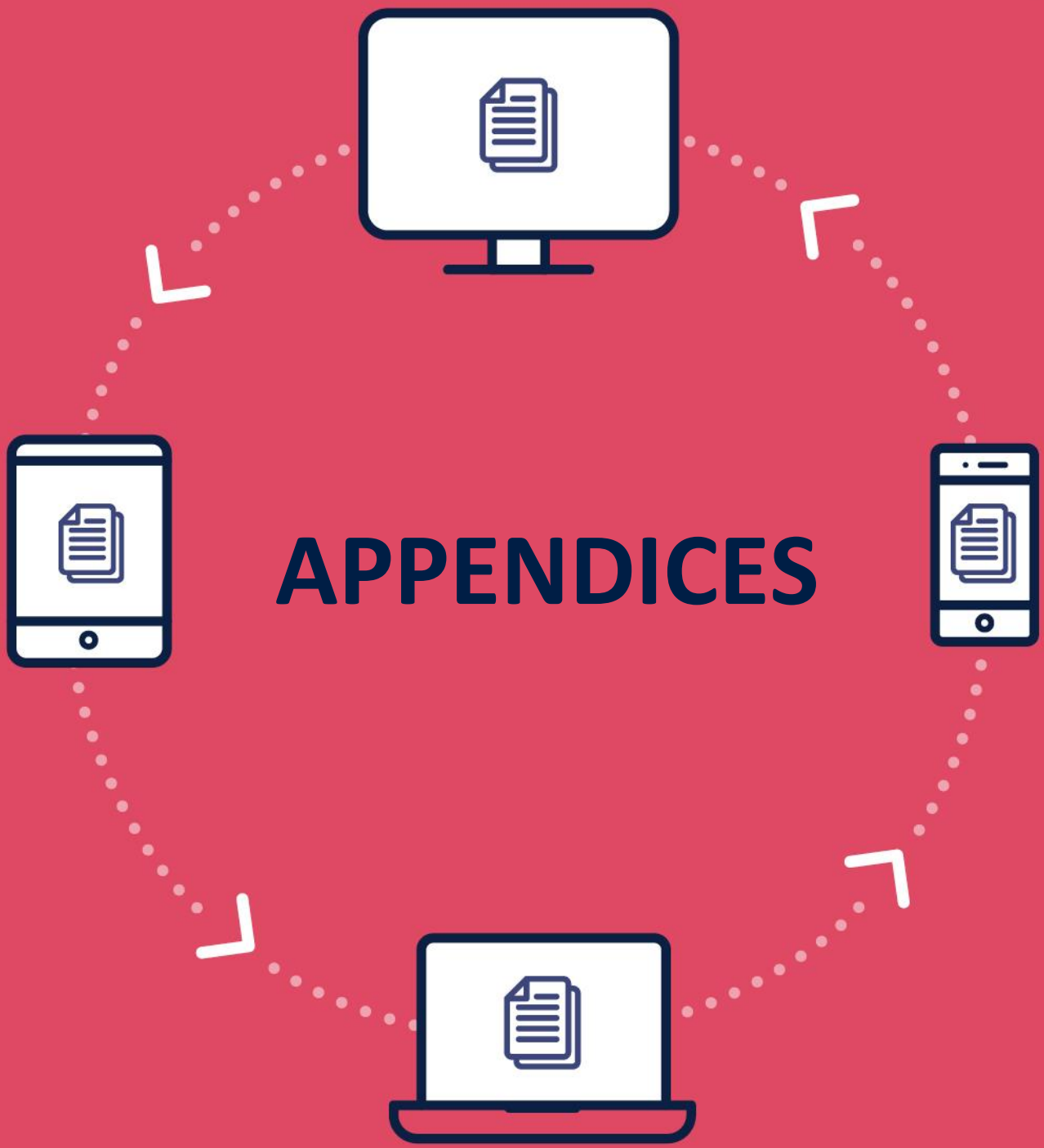
14.2. Update and Test Cyber Incident Response Plan

The PIR may result in changes to the CIRP, Playbooks and Templates. Changes should be communicated to the relevant personnel.

14.3. Training

All employees of the company should undergo Cyber Security Awareness training. This training should encompass how to identify and combat cyber security threats. A broad overview should be given of the methods that cyber attackers used to target employees such as weak authentication and session management. It should also cover access controls, phishing and the risks and weaknesses associated with these attacks. The training should also provide mechanisms to protect data.

Employees should also be required to undertake Cyber Incident Response training to gain an understanding of how incidents are handled and the technical skills required to manage these threats.



APPENDICES

Appendix A

Terminology and Definitions

Use of consistent and pre-defined terminology to describe incidents and their effects can be helpful during a response. In your CIRP, include commonly used terms used in your organisation. ACSC defines cyber threats, events, alerts and incidents as follows:

Cyber threat

A cyber threat is any circumstance or event with the potential to harm systems or information. Other threats are listed on cyber.gov.au. Organisations can include a list of cyber threats of concern. The ACSC Annual Cyber Threat Report (2021) outlines the following threat environment and key cyber security trends:

- COVID-19 themed malicious activity including phishing emails and scams
- Ransomware
- Exploitation of security vulnerabilities
- Software supply chain compromise
- Business Email Compromise
- Cybercrime

Cyber security event

A cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

A cyber security event has the potential to become, but is not confirmed to be, a cyber incident.

Examples of cyber security events include (but are not limited to):

- A user has disabled the antivirus on their computer
- A user has deleted or modified system files
- A user restarted a server
- Unauthorised access to a server or system.

Cyber security alert

A cyber security alert is a notification generated in response to a deviation from normal behaviour. Cyber security alerts are used to highlight cyber security events.

Cyber incident

A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations. A cyber incident requires corrective action.

Examples of cyber security incidents include (but are not limited to):

- Denial-of-service attacks (DoS)
- Unauthorised access or attempts to access a system
- Compromise of sensitive information
- Virus or malware outbreak (including ransomware).

Appendix B

Cyber Incident Response Readiness Checklist

This checklist is to aid your organisation's initial assessment of its readiness to respond to a cyber security incident. This checklist is not an exhaustive list of all readiness activities.

PREPARATION	
☐	Your organisation has a cyber security policy or strategy that outlines your organisation's approach to prevention, preparedness, detection, response, recovery, review and improvement. • For example, does your organisation have a position on, for example, paying ransom, reporting incidents to government, publicly acknowledging cyber incidents, sharing information about incidents with trusted industry and government partners?
☐	A Cyber Incident Response Plan has been developed, which: • Aligns with your organisation's operating environment and other processes, including emergency management and business continuity processes. • Has been reviewed or tested in an exercise to ensure it remains current and responsible personnel are aware of their roles, responsibilities and processes. • Templates have been prepared, for example Situation Reports.
☐	Staff involved in managing an incident have received incident response training.
☐	Up-to-date hard copy versions of the Cyber Incident Response Plan and playbooks are stored in a secure location (in case of electronic or hardware failure) and are accessible to authorised staff members.
☐	Specific playbooks to supplement the Cyber Incident Response Plan have been developed, that define step-by-step guidance for response actions to common incidents, and roles and responsibilities.
☐	A Cyber Incident Response Team (CIRT) and a Senior Executive Management Team (SEMT) – or equivalents - have been formed to manage the response, with approved authorities.
☐	All relevant IT and OT Standard Operating Procedures (SOPs) are documented and have been reviewed or tested in an exercise to ensure they remain current and responsible personnel are aware of their roles, responsibilities and processes.
☐	Arrangements for service providers, including cloud and software as a service, to provide and retain logs have been established and tested to ensure these include useful data and can be provided in a timely manner.
☐	Log retention for critical systems have been configured adequately and tested to confirm that they capture useful data. Refer to the ACSC publications including Windows Event Logging and Forwarding for specific guidance.
☐	Your organisation has internal or third party arrangements and capabilities to detect and analyse incidents. If these capabilities are outsourced, your organisation has an active service agreement/contract.

☐	Critical assets (data, applications and systems) have been identified and documented.
☐	Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for use of facilities and communications technologies in response to cyber incidents, and these resources are confirmed as available. This includes for alternative/back-up ICT-based channels.
☐	Incident logging/records and tracking technologies used to manage a response are confirmed as available and have been tested.
☐	Role cards have been developed for each person involved in the CIRT and the SEMT. Individual actions will depend on the type and severity of the incident. Example role card is available at Appendix J.
☐	Your organisation has internal or third party arrangements and capabilities to monitor threats. Situational awareness information is collected from internal and external data sources, including: • Local system and network traffic and activity logs • News feeds concerning ongoing political, social, or economic activities that might impact incident activity • External feeds on incident trends, new attack vectors, current attack indicators and new mitigation strategies and technologies.
DETECTION, INVESTIGATION, ANALYSIS AND ACTIVATION	
Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for:	
☐	Detection mechanisms which can be used to identify potential information security incidents, such as scanning, senses and logging mechanisms. These mechanisms require monitoring processes to identify unusual or suspicious activity, for example behaviour and logging, commensurate with the impact of an incident. Common monitoring techniques include: a) network and user profiling that establishes a baseline of normal activity which, when combined with logging and alerting mechanisms, can enable detection of anomalous activity; b) scanning for unauthorised hardware, software and changes to configurations; c) sensors that provide an alert when a measure breaches a defined threshold(s) (e.g. device, server and network activity); d) logging and alerting of access to sensitive data or unsuccessful logon attempts to identify potential unauthorised access; and e) users with privileged access accounts subject to a greater level of monitoring in light of the heightened risks involved.[1]
☐	Incident detection, including self-detected incidents, notifications received from service providers or vendors, and notifications received from trusted third parties (e.g. ACSC).
☐	Incident analysis, including how incidents are to be categorised, classified and prioritised, and controls related to how data is stored and transmitted (i.e. if out-of-band transmission is required).
☐	Activating a Cyber Incident Response Team (CIRT) to manage critical incidents, with roles and responsibilities assigned.

[1] APRA Prudential Practice Guide CPG 234 Information Security.

☐	Activating a Senior Executive Management Team (SEMT) to manage critical incidents, with roles and responsibilities assigned.
CONTAINMENT, EVIDENCE COLLECTION AND REMEDIATION	
☐	Standard Operating Procedures (SOPs), playbooks and templates, have been developed, and roles and responsibilities assigned for containment, evidence collection and remediation. These can be included as appendices to the Cyber Incident Response Plan.
☐	A secure location is available for storing data captured during an incident, which could be used as evidence of the incident and the adversary's tradecraft, and ready to be provided to third-party stakeholders if needed.
COMMUNICATIONS	
☐	Policy, plans, Standard Operating Procedures (SOPs) and templates have been developed to support communicating with: • Internal stakeholders (e.g. Board, staff) • External stakeholders (e.g. stakeholders to assist with the response and stakeholders with an interest in the response)
☐	Policy, plans, Standard Operating Procedures (SOPs) and templates for media and communications professionals have been developed, and roles and responsibilities assigned, to support public and media messaging.
☐	You organisation has assigned a public and media spokesperson, who is supported by subject matter experts.
☐	Staff have been trained to implement the communications processes and execute their roles and responsibilities.
☐	Staff who are not involved in managing incidents are cognisant of your organisation's policy and processes and their responsibilities when an incident occurs (e.g. exercising discretion, using approved talking points, referring enquiries to the designated officer).
INCIDENT NOTIFICATION AND REPORTING	
☐	Processes and contact details are documented to support the organisation to meet its legal and regulatory requirements on cyber incident notification, reporting and response, with roles and responsibilities within your organisation are assigned. This includes the processes for obtaining authority to release and share information.
☐	Processes are documented for insurance requirements.
POST INCIDENT REVIEW	
☐	A process is documented to conduct Post Incident Reviews (PIR) following conclusion of an incident and PIR reports with recommendations are submitted to management for endorsement.
☐	A process is documented to ensure actions following incidents and/or exercises are tracked and completed (e.g. Action Register).

Appendix C

ACSC Incident Triage Questions

Where applicable, personnel reporting cyber security incidents to the ACSC on behalf of their organisation should try to have information available to answer the following questions:

- Who is reporting the incident? (include their position e.g. CISO, ITSA, SOC Manager etc.)
- Who/what is the affected organisation/entity?
- What type of incident is being reported? (e.g. ransomware, denial of service, data exposure, malware)
- Is the incident still active?
- When was the incident first identified?
- Are you reporting for ACSC awareness or is ACSC assistance required?
    - If ACSC assistance is required, what assistance is needed?
- What type of system or network has been affected?
    - Information Technology (IT)
        - Corporate systems/networks, databases, servers, VOIP systems.
    - Operational Technology (OT)
        - SCADA, Remote sensors, BMS/BAS, logic controllers.
- What was observed (the sequence of events)? E.g. was lateral movement observed?
    - Date/Time
    - Effect/Event
- Who or what identified the problem?
- Has a data breach occurred?
    - What type of information was exposed?
        - What impact will this have on the organisation?
        - What impact (if any) will the breach have on public safety or services?
    - What volume of records/data was exposed?
    - Was it a misconfiguration/error, or was a malicious exfiltration or theft of data identified?
    - Has it been reported to the Office of the Australian Information Commissioner (OAIC)?
        - If not, organisations need to consider if mandatory reporting obligations apply under the Notifiable Data Breach (NDB) scheme
- What actions have been taken to rectify the issue?
    - Does the organisation/entity have internal or external IT and/or cyber security incident response providers?
    - Are services/business as usual operations interrupted?
        - If so, how long do they expect before they are back at normal operating capability?
- Will you be communicating publicly about the incident and engaging with media?
    - If so, please notify the ACSC beforehand if you will be referencing the ACSC.

Appendix D

Situation Report Template

Date of entry:	Time of entry:	Author:
Date and Time incident detected		
Current Status – New, In Progress, Resolved		
Incident Type		
Incident Classification		
Scope – list the affected networks, systems and/or applications; highlight any change to scope since the previous log		
Impact – list the affected stakeholder(s); highlight any change in impact since the previous log entry		
Severity – outline the impact of the incident on your organisation(s) and public safety or services; highlight any change to severity since the previous log entry		
Notifications Actioned/Pending		
Assistance required – what assistance do we require from other organisations? (e.g. ACSC, law enforcement)		
Actions taken to resolve incident		
Additional notes		
Contact details for incident manager and others if required		
Date and Time of next update		

Appendix E

Incident Log Template

Date and Time	Notes (relevant facts, decisions, rationale)

Appendix F

Evidence Register Template

Date, Time and Location of collection	Collected by (name, title, contact and phone number)	Item Details (quantity, serial number, model number, hostname, media access control (MAC) address, IP addresses and hash values)	Storage location and label number	Access

Appendix G

Remediation Action Plan Template

Date and Time	Category (Contain, Eradicate, Recover)	Action	Action Owner	Status (unallocated, In Progress, Completed)

Appendix H

Post Incident Review Analysis Template

Incident Summary

Incident name	
Date of incident	*dd/mm/yy*
Incident Priority	*Low/Medium/High* *Established from the impact and/or risk to the business*
Time incident occurred	
Time incident was resolved	
Incident type	*Malware, etc.*
Personnel involved	*Names of the individuals involved in resolving the incident and their function(s), including any service providers*
Incident impact	*What impact did the incident have? I.e. loss of systems*
Brief summary	*What happened?*

Incident Analysis

The Incident Analysis is broken into the following categories:

- **Incident timeline** – Summary of what happened and when. Provides high level areas for improvement.
- **Protection** – Identifies the protection mechanisms that were in place at the time of the incident and their effectiveness. Establishes how to improve the protection of our systems and networks.
- **Detection** – Establishes how to reduce the time to identify an incident is occurring. Addresses what detection mechanisms were in place, and how those mechanisms can be improved.
- **Response** – Identifies improvements for the incident response.
- **Recovery** – Addresses improvements for incident recovery (i.e. how to recover from an incident faster).

INCIDENT TIMELINE	
Date and time of detection	
When was the incident acknowledged?	*When did your organisation identify that an incident was occurring?*
Date and time of incident response	
Date and time of incident recovery	
Who discovered the incident first and how?	*Or who was alerted to it first? How did the discovery or alert happen?*
Was the incident reported externally? If yes, when?	*For example, did your organisation report it to the ACSC?*
Who supported resolving the incident? When did they provide support?	*List the names of personnel involved in resolving the incident, and the time (and date if not all on the same day) they joined in.*
What activities were conducted to resolve the incident? When were they conducted and what was their impact?	*It is easier to do this in a list, for example:* *Time > Task > Impact*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

PROTECTION	
What controls were in place that were expected to stop an incident similar to this?	*I.e. systems, networks, etc.*
How effective were those controls?	*Did they work? Why/why not?* *How could they be improved?*
Are there other controls considered better for protecting against a similar incident?	*What are they?*
What business processes were in place to prevent this type of incident from occurring?	*I.e. Your organisation's policies and procedures.*
How effective were those business processes?	*Did they work? Why/why not?* *How could they be improved?*
Any other findings and/or suggestions for improvement?	***See the PPOSTTE model for guidance*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

INCIDENT DETECTION	
How was the incident detected?	*How did you know the incident was happening?*
What <u>controls</u> were in place to detect the incident?	
Were those <u>controls</u> effective?	*Did they work? Why/why not?*
What <u>business processes</u> were in place to detect the incident?	
Were those <u>business processes</u> effective?	*Did they work? Why/why not?*
Are there any ways to improve the 'time-to-detection'?	*How could your organisation reduce that time?*
Are there any indicators that can be used to detect similar incidents in the future?	
Are there any additional tools or resources that are required in the future to detect similar incidents?	*Is there anything (from a detection perspective) that will help mitigate future incidents?* *Technology? Human resources with specific skills? Etc.*
Any other findings and/or suggestions for improvement?	*What activities worked well? What activities did not work so well? What could be changed with hindsight?* ***Also see the PPOSTTE model for guidance*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

INCIDENT RESPONSE	
What was the cause of the incident?	
How was the incident resolved?	*What needed to happen for the issue to be resolved?*
What obstacles were faced when responding to the incident?	
Were any business policies and/or procedures used in responding to the incident?	*For example, does your organisation have an Incident Response Plan, and was this followed?*
Were those business policies and/or procedures effective?	*Did they work? Why/why not?*
What delays and obstacles were experienced when responding?	
Were there any escalation points?	*Were there any escalation points that the incident went through?*
If there were escalation points, did they hamper the response OR were they at the appropriate level?	*For example, having to escalate to a Chief Operating Officer (COO) to take action on an ongoing incident had severe timeline impacts on responding to an active incident.*
How well did the information sharing and communications work within your organisation?	*What worked well/what did not work well. How could it be improved?* *Was there any information that was needed sooner?* *How did your organisation communicate within the IR team, across jurisdictions, across time zones, legal teams, external comms teams, etc.?*
Were there any media enquiries received during the incident?	*If yes, WHAT was the media, and how did your organisation respond?*
Was media produced during the incident?	*If yes, WHAT was the media, and how did your organisation respond?*
Was the customer notified during the incident?	*Why/why not? When? How?*
Were trained staff available to respond?	*Are there any staff knowledge and/or skills gaps? What are they?* *Were there enough resources available to respond?*
Any other findings and/or suggestions for improvement?	***See the PPOSTTE model for guidance*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

INCIDENT RECOVERY	
How long did it take for all systems and networks to recover?	
How could this time be improved?	*For example, how could the recovery time be reduced?*
Are there any obligations to report externally about the incident?	
Were there any media enquiries after the incident?	
Were staff and/or customers notified of the incident?	*Why/why not?* *How was the notification completed? Was it effective? How could it be improved?*
Any other findings and/or suggestions for improvement?	***See the PPOSTTE model for guidance*
PROPOSED ACTIONS	*Detail any resulting actions that can be incorporated into the Action Register.* *Brief description of action > Proposed Action Officer*

Appendix I

Action Register Template

ID	Action	Action Officer	Date expected to complete	Status	Updates	Comments
01	*Describe the action in detail*	*Name of the person who will be leading the action*	*Date the action is expected to be completed*	*Complete* *In Progress* *Not yet started*	*Insert date, and any updates to progressing the action* *You can also detail any blockers here*	*Any relevant information relating to closing out he action*
02						
03						
04						
05						

Appendix J

Role Cards

Example of a role card:

ROLE CARD – CYBER INCIDENT RESPONSE

INCIDENT MANAGER

Reports to SEMT Chair

RESPONSIBILITIES

- Activate the CIRP
- Coordinate operations room setup
- Manage a team of incident responders including preparing for, and tracking, daily investigation tasks
- Provide administrative and logistical support for incident responders
- Manage the passage of relevant operational information to the SEMT

ROLE CARD – CYBER INCIDENT RESPONSE

KEY CONTACTS

Virtual Meeting Room:
XXXX

Backup conference line:
XXXX

Media:
XXXX

Security:
XXXX

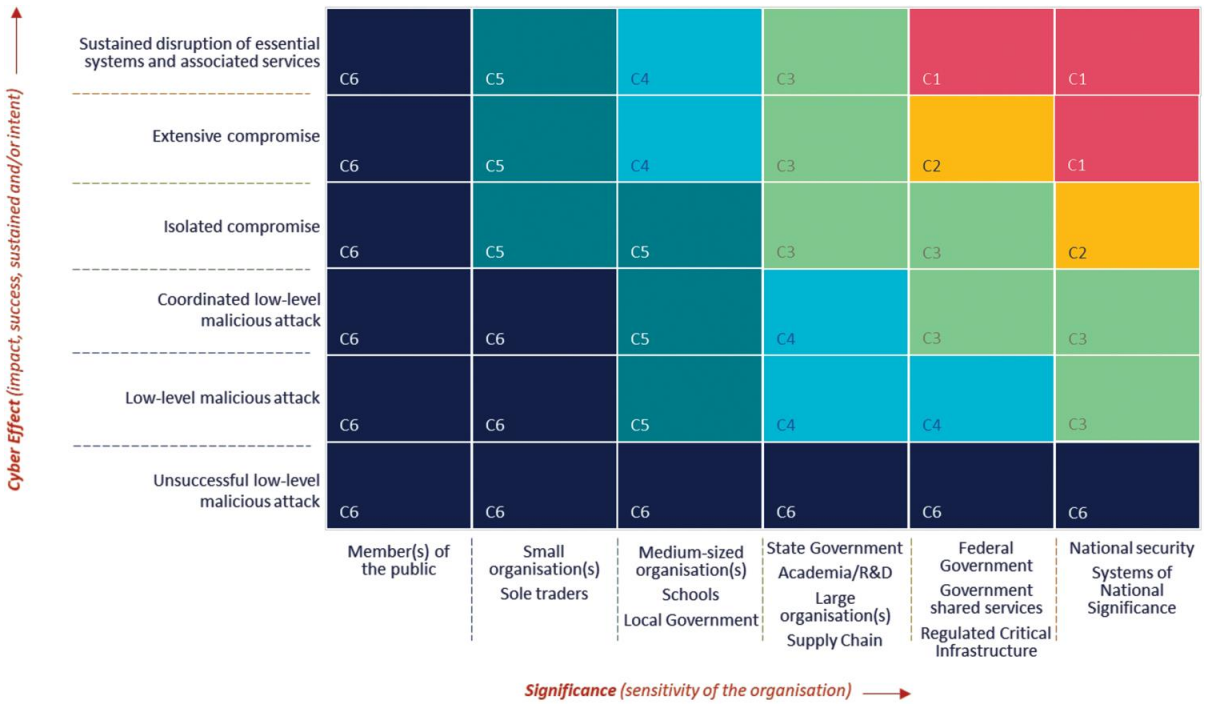
Legal:
XXXX

Appendix K

ACSC Incident Categorisation Matrix 2022

ACSC categorises cyber incidents by severity using a matrix that considers the:

- Cyber Effect (i.e. the impact, success, sustained and/or intent)
- Significance (i.e. sensitivity of the organisation)



The severity of the cyber incident informs the type and nature of incident response and crisis management arrangements that are activated. Depending on the severity of the incident, the ACSC has a suite of capabilities that it may deploy to support the affected parties. However, ACSC determines which capabilities are appropriate and available given competing priorities. Organisations must not rely on the ACSC for their own ability to respond to cyber incidents in an appropriate and timely manner.

Appendix L

CIRT Team as of 2 December 2023

Points of Contact for Reporting Cyber Incidents

Primary and secondary (backup) internal points of contact to report cyber incidents to over a 24/7 period.

Name	Hours of Operation	Contact Details	Role Title	Responsibilities
Indiah Smith	9:00am-5:30pm	irsmith@deakin.edu.au	Cyber Security Policy Advisor	Creating, reviewing and assessing policies and procedures and overseeing risk management.

Cyber Incident Response Team (CIRT)

CIRT members responsible for managing responses to cyber incidents:

Name	Organisation Role	Contact Details	Hours of Operation	CIRT Role Title	CIRT Responsibilities
Joel Daniel	Cyber Security Team Leader	s219504809@deakin.edu.au	9:00am-5:30pm	Team Leader	Coordinates activities of the incident response team, and the focus of the team in minimising damage and facilitating recovery
Asseel Mala	Senior Cyber Security Team Member	awmala@deakin.edu.au	9:00am-5:30pm	Lead Investigator	Collects and analyses evidence for the purpose of determining the issue and implementing appropriate recovery mechanisms
	Senior Cyber Security	rgimolli@deakin.edu.au	9:00am-5:30pm		Coordinates communication efforts with

Rinor Gimolli	Team Member			Communications Lead	internal and external stakeholders
Melvin Manoj	Senior Cyber Security Team Member	mmanoj@deakin.edu.au	9:00am-5:30pm	Documentation and Timeline Lead	Logging team activities and engaging in record keeping of investigation and recovery tasks on an incident timeline
Mallikarjuna Reddy Karasani	Junior Cyber Security Team Member	s223099546@deakin.edu.au	9:00am-5:30pm	HR Representative	Responsible for providing support to employees and the communication is effective and compliant with company policy

For more significant cyber security incidents the CIRT could be expanded to include:

Name	Organisation Role	Contact Details	CIRT Role Title	CIRT Responsibilities
Ramya Sekar	Company Leader	s222569052@deakin.edu.au	Company Leader	Responsible for ensuring the incident is communicated, documented or escalated effectively
Duc Thanh Nguyen	Company Acting Director	duc.nguyen@deakin.edu.au	Company Director	Responsible for supporting critical decision-making

SEMT Team as of 2 December 2023

Senior Executive Management Team (SEMT)

SEMT members responsible for managing responses to cyber incidents:

Name	Contact Details	Title	SEMT Role

Ramya Sekar	Company Leader	s222569052@deakin.edu.au	Responsible for ensuring the incident is communicated, documented or escalated effectively
Duc Thanh Nguyen	Company Acting Director	duc.nguyen@deakin.edu.au	Responsible for supporting critical decision-making