Incident Response Plan

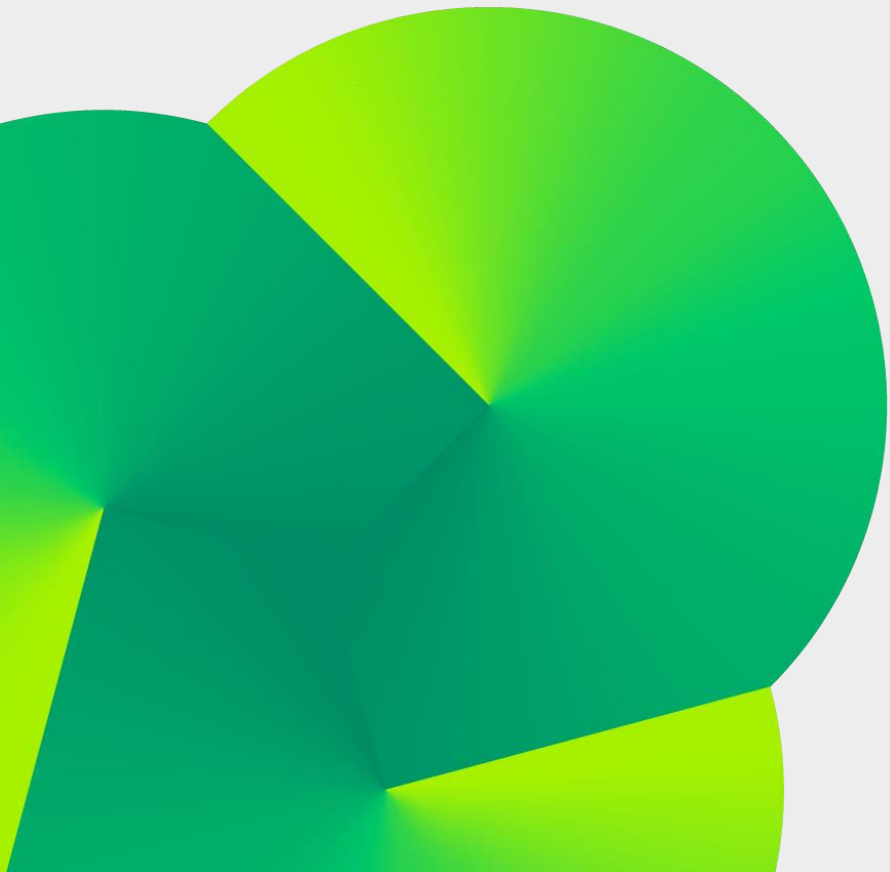
Example

Prepared For

Community Housing Industry Association NSW (CHIA NSW)

Version 0.1

11/07/2022



Contents

1 Introductions 3
1.1 Purpose 3
1.2 Recognised Industry Guidance 3
1.4 Objectives 3
1.5 Scope Inclusions 4
1.6 Scope Exclusions 4
1.7 Strategy 4
2 Definitions 7
3 Elements 7
3.2 Incident Severity Ratings 7
3.3 System Recovery Rating 8
3.4 Incident Response and Extended Incident Response Team Membership 9
3.5 Incident Response – Allocation of Roles and Responsibilities 9
4 Incident Ownership 10
5 Authorisation for Immediate Action 11
6 IT Tools and Systems Consideration 11
7 Response Procedures 13
7.1 Preparation 13
7.2 Incident Detection and Reporting 14
7.3 Initial Triage Analysis 15
7.4 Containment 16
7.5 Evidence Collection 18
7.6 Analysis and Reporting 19
7.7 Eradication 21
7.8 Recovery 23
7.9 Post Incident Analysis 24
Appendix A – Communications Plan 26
Appendix B – Reporting Obligations 29
Appendix D – Contact Details 31

Acknowledgement

CHIA NSW would like to acknowledge the funding provided by the NSW Department of Communities and Justice (DCJ) to support the development of this resource under the NSW Community Housing Industry Development Strategy. The NSW Community Housing Industry Development Strategy is a partnership between CHIA NSW and DCJ.

1 Introductions

1.1 Purpose

The Community Housing Provider (CHP) recognises the importance of the security over its systems, information and data stores. CHP processes client and corporate data sets which are deemed confidential (Confidentiality) and critical to the continuation of its business operations. Community Housing Industry Association's information sources and systems are required to be accurate (Integrity) and highly available (Availability) and accordingly has process and technical mechanisms in place to protect those critical systems and data.

However, CHP recognises that despite preventative controls being implemented across the network, systems and data threats to these systems exist and that incidents, cyber initiated or otherwise could occur that compromise the confidentiality, integrity and availability of those systems data.

This Incident Response Plan is designed to prepare all CHIA NSW Members for any such incident and is used to guide the response actions when preparing, detecting, analysing, investigating, managing, recovering and reporting information security incidents.

1.2 Recognised Industry Guidance

This plan has been developed based on structures and principles defined across a number of industry recognised frameworks for incident response and contextualised for the operations of CHIA NSW and its Members. In developing this incident response plan, we have considered and applied relevant guidance from the following sources.

- NIST 800-61 Revision 2 – Computer Security Incident Handling Guide
- ISO/IEC 27035:2011 – Information Security Incident Management
- CERT: Handbook for Computer Security Incident Response Teams (CSIRTs)
- ISACA – Incident Management and Response – Based on COBIT 5

1.4 Objectives

The core objectives of the Incident Response Plan are:

- Provide standard and tested processes to be used for the efficient response, analysis/investigation, recording, management and reporting of incidents.
- Provide structured communication and stakeholder management protocols for use during and post the detection of any incident requiring a formal response.
- Enhance stakeholder perception of IT though a consistently professional approach to communicate incidents when they occur and restore services quickly to minimise harm to
- Improve future response to incidents by learning and adapting response procedures from the analysis of handling of prior incidents.

1.5 Scope Inclusions

The scope of this plan includes all information security incidents that have the potential to breach the security of information over which CHP have responsibility to protect. This includes incidents affecting:

- Internal information systems of CHP
- Information external service providers manage, store or process on behalf of the CHP

- All privacy information and personally identifiable information stakeholders provide to CHP
- All related data stored or processed by or on behalf of CHP

This plan applies to all CHP employees, contractors and others with access to the CHP information systems. External parties supplying information and communication technology services to CHP are expected to support information security incident responses and activities through suitable clauses in their contracts with CHP

1.6 Scope Exclusions

The plan explicitly excludes incidents involving the following:

- Information CHP was obliged to provide to external organisations under legislation such as to government departments;
- Information technology management and administration activities where the risks to information were identified and suitable contingency plans developed; and
- Known problems and issues that are being managed.

1.7 Strategy

The incident response plan relies on CHP personnel having the ability to contain incidents and complete some basic analyses of incidents to decide whether the incident:

- Can be managed internally or requires the assistance of specialist service providers;
- Needs to be reported under legislative, regulatory or contractual requirements;
- Should be reported to law enforcement agencies;
- Requires a during or post-incident assessment to uncover root causes, and if necessary, improved information security protective mechanisms or the incident response plan.

The general steps for information security incident response are outlined in the table below.

Stage	Activities	Responsibility
Preparation	• Setup an information security response team and documentation to handle various types of incidents. • Establish liaison with organisations who may be called upon to support response activities. • Prepare information systems for responding to incidents such as recording event logs. • Install analysis and response tools as required to complete response plans efficiently. • Train staff as appropriate in the response to incidents.	IT staff
Detect	• Monitor IT systems and assets and report any suspicious activities or evidence of an information security incident	All staff and IT users
Analyse	• Confirm that an incident has occurred, determine the scope of the incident and the potential severity of the incident. • Prioritise incidents and actions requirement to contain incident. • Escalate incident as required.	All IT staff
Containment	• Act as appropriate to limit harm to CHP and its clients. • Contact support staff and support organisations if assistance is likely to be required.	All IT staff
Evidence Collection and analysis	• If warranted, collect and secure evidence to allow the incident to be fully analysed or used in legal proceedings. • Analyse data and determine complete scope of incident. • Formulate a plan to recover to normal operations and estimate the time and resources for recovery.	Incident Response Team
Eradication	• Address the source of the problem to ensure that the incident is stopped. • Remove malware, corrupted data, any installed backdoors access mechanisms • Confirm that systems and data have been secured.	Incident Response Team
Recovery	• Recover as much of the lost IT systems and data as is practical. • Complete user acceptance testing to confirm successful recovery • Report to business leaders the data lost that must be re-entered or worked arounds or recovered manually. • If necessary, increase monitoring to protect assets.	All IT staff
Post Event Analysis	• Complete a review of the incident to determine the root causes, identify and assess potential improvements to IT systems, policies and procedures, and recommend changes that are justified. • Create a closing report and present findings and recommendations	Incident Response Team

Table 1 – Incident Response Overview

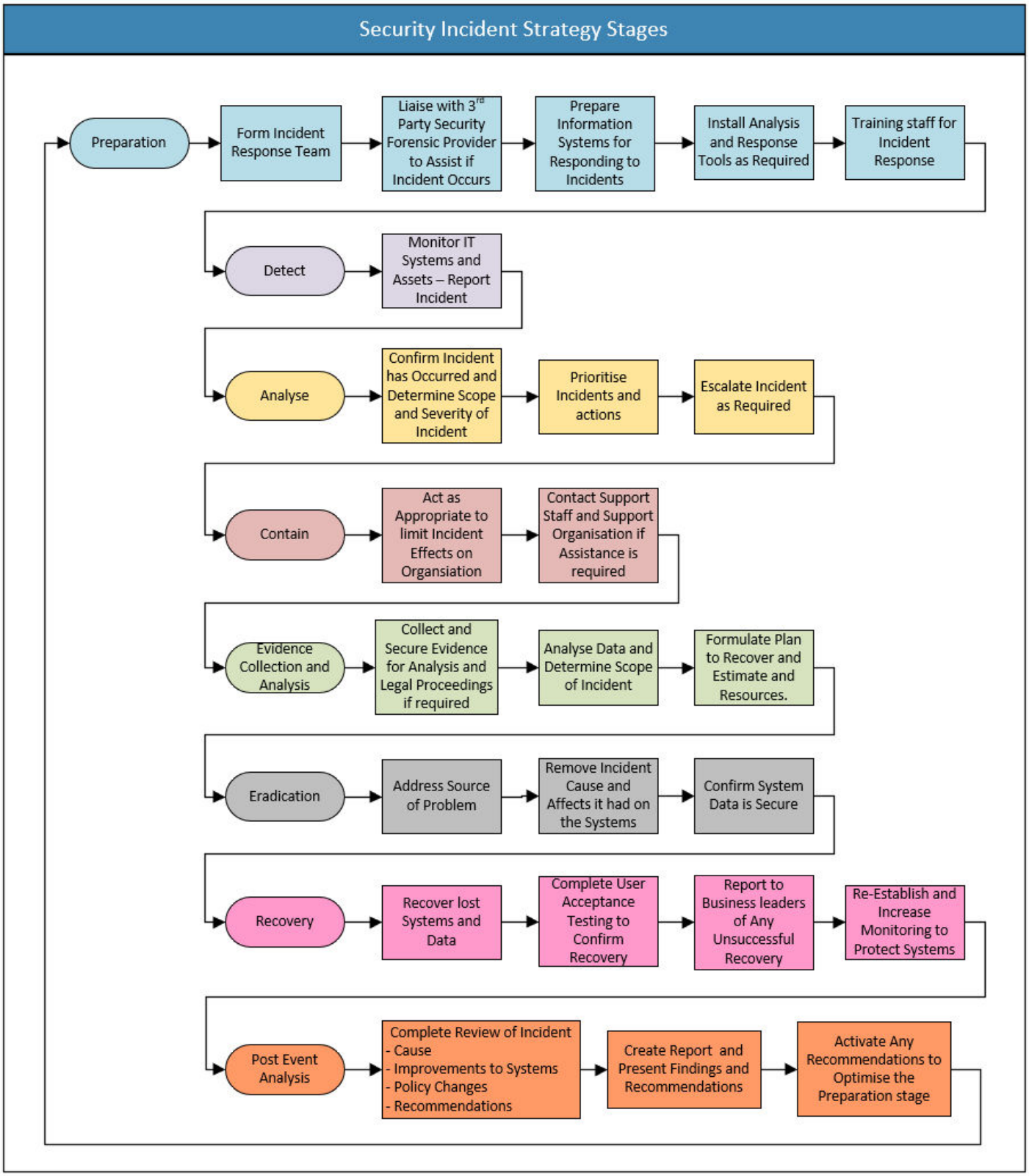


Table 2 – Incident Response Strategy Stages

2 Definitions

Terminology	Definition
Configuration Item	A subset of service assets that have a direct impact on service delivery and need to be managed to deliver an IT service. These items are configurable and managed through Change Management.
Incident	An unplanned event that disrupts or reduces the quality of an IT service (or threatens to).
Major Incident	An incident with significant business impact that requires immediate coordinated resolution
Problem	An unknown root cause with the potential to or that is causing one of more Incidents.
Stakeholder	A person or group of people affected by an incident or can influence mitigation decisions, either as a consumer or provider.
Information Security Incident	An event or series of events that could compromise the confidentiality, integrity or availability of CHP information or information systems.
Crisis Management Team	A crisis management team, also known as a CMT, incident management team, or corporate incident response team, prepares an organisation to respond to potential emergencies. It also executes and coordinates the response in the event of an actual disaster.

3 Elements

3.2 Incident Severity Ratings

Information security incidents have the potential to cause serious harm to CHP through:

- Disruption of services necessary to complete business process;
- Loss of information and effort to recreate the information or reprocess data;
- Corruption of data and information systems resulting in the need to restore data from backups and loss of some data;
- Information being exfiltrated and/or used without authorisations harming Community Housing Industry Association, Clients and staff;
- Increased time and costs for responding to incidents;
- Legal and/or regulatory actions; and
- Damage to Community Housing Industry Association's reputation.

Rate incidents according to the highest category that applies according to the following Table.

Rating	Characteristic
Critical	• The incident has the potential to disclose bulk privacy information and/or critical business information OR • The incident has the potential for sensitive information to be disclosed that could cause major harm to CHP and its Clients, OR • The incident could result in major fraud, OR • The incident could result in information systems being unavailable for an extended period (more than 2 business days or beyond the systems recovery time objective), OR • The incident indicates systemic problems with mechanisms protecting information systems, OR • There is potential for media or government or regulator interest in the incident
Serious	• The incident has the potential to reveal limited privacy information but not critical business information, OR • The incident has the potential for sensitive information to be disclosed that could cause some harm to CHP, which could be readily managed, and costs absorbed, OR • The incident could result in limited fraud, OR • The incident could result in critical information systems being unavailable and requires workarounds to be initiated (an expected outage of more than 8 hours, or up to the recovery time objective)
Routine	• The incident is unlikely to disclose privacy or critical business information, result in fraud, OR • Is unlikely to result in an extended IT system outage (no more than 8 hours and within the Recovery Time Objective).

Table 3 – Incident Ratings

3.3 System Recovery Rating

The System availability impact rating is used to determine if disaster recovery procedures need to be enacted to ensure that normal business process continues. If it is decided to action the disaster recovery procedures, it should be determined that the incident will not impact the process.

Rating	Characteristic
Delayed	Recovery of an information system is expected to take longer than the recovery time objective
Acceptable	Recovery of an information system is expected to be completed within its recovery time objective.
Routine	Systems are expected to be available within 8 hours and within the recovery time objective

Table 4 – Incident Ratings

3.4 Incident Response and Extended Incident Response Team Membership

The Incident Response Team (IRT) within CHP comprises relevant areas and personnel across the business with a vested interest in the management and response to cyber and other incidents. The current IRT membership consists of the following:

Incident Response Team			
Functional Area	**Name**	**Position**	**Primary / Secondary**
Information Technology	<Insert Name of Person>	<Insert Position Title>	Primary
Information Technology	<Insert Name of Person>	<Insert Position Title>	Primary
Information Technology	<Insert Name of Person>	<Insert Position Title>	Secondary
Information Technology	<Insert Name of Person>	<Insert Position Title>	Secondary
Operations	<Insert Name of Person>	<Insert Position Title>	Primary

Table 5 – Incident Response Team

3.5 Incident Response – Allocation of Roles and Responsibilities

Incidents that are rated serious or critical must be escalated to the incident response team. The incident response team will assume responsibility for analysing, responding to, reporting and managing the overall response. The team member and their roles are specified in the following table

Role	Assigned to	Responsibilities
Incident Response Lead (IRL)	<Insert Position Title>	• Provide management and oversight • Seek advice from other subject matter experts (e.g., human resources and legal) as required • Decide if law enforcement or other organisations need to be informed of the incident • Liaison with Crisis Management Team if required
Incident Response Coordinator	<Insert Position Title>	• Manage the operational deployment of resources in consultation with the IRL • Oversight the technical actions throughout the incident • Complete allocated technical tasks to investigate incidents and report on details of incidents and their implications • Advise action to take to eradicate attacks and recover systems • Manage evidence • Record actions taken and findings
Log Keeper	As Delegated	• Record decisions and actions taken
Technical Response Coordinators	<Insert Position Title>	• Allocate staff and resource to response activities involving IT • equipment • Liaise with IT support staff and external IT service providers for managing the incident

Role	Assigned to	Responsibilities
		• Decide, authorise and direct technical activities
Business Response Coordinator	<Insert Position Title>	• Allocate staff and resources to non-IT systems response activities, such as facilities management and physical security • Assess incident to determine if action is required for regulatory or compliance purposes, considering Community Housing Industry Association's policies, procedures and risk tolerances, data protection and the Australian Privacy Act • Decide, authorise and direct non-technical activities
Specialist Advisory Service	Incident Response Team	• Provide technical guidance for responding to incidents
Business Advisor	<Insert Position Title>	• Provide advice regarding business impact of breach and actions to take minimise harm • Manage evidence • Record actions taken and findings
Communications	<Insert Position Title>	• Prepare briefings and reports to crisis management team, media, affected staff and clients as appropriate • Prepare and present a consistent response to media and stakeholders for major incidents
Privacy Officer	<Insert Position Title>	• Determine if the incident has scope for serious harm to affected individuals • Decide if the actions taken renders the possibility of serious harm to affected individuals unlikely • If necessary, advise on disclosure requirements under the Notifiable Data Breaches amendments to the Privacy Act

Table 6 – Incident Response Team Responsibilities

4 Incident Ownership

The incident owner is responsible for managing the incident including:

- Documenting the incident and actions taken to respond to the incident;
- Advising the information systems owners of affected systems of the incident and progress for controlling the incident;
- Investigating the incident and assessing the potential impact;
- Escalating incident and handing over incident as required; and
- Taking actions to control the incident

The person acting in the incident owner role depends on the severity of the incident according to the following table:

Incident Severity Rating	Incident Type	Incident Owner
Critical	All Information security incidents	Incident Response Team (headed by the Incident Response Lead)
Serious	Cyber Security Incidents	<Insert Position Title>
Serious	Other Incidents	<Insert Position Title>
Routine	Cyber Security Incidents	<Insert Position Title>
Routine	Other Incidents	<Insert Position Title>

Table 7 – Incident Ownership and Responsibility

5 Authorisation for Immediate Action

The Incident Owner Coordinator, and Incident Response Team as appropriate are authorised to take any immediate action they deem necessary to contain information security incidents provided that:

- The matter is urgent to protect CHP assets or interests; and

- A delayed response is likely to lead to increased harm; and
- Seeking explicit authorisation is likely to cause unacceptable delays or is impractical; and
- A report of the incident and actions taken (highlighting actions beyond normal authorisation) are sent to the Manager as soon as practical following the action being taken
- IT staff to only be able to run pre-defined or pre-determined tasks. Business services can only be shut down by a member of the Incident Response Team upon executive or management approval, and a retrospective Change Control process must be conducted

The authority includes confiscating or disconnecting equipment, monitoring suspicious activity, powering down IT equipment (consider any forensic investigation requirements that may be relevant), and remote wiping of mobile devices.

6 IT Tools and Systems Consideration

A major attack on IT systems can create difficulties for analysing incidents, tracking incident and sharing information. To ensure that the incident response is efficient and timely, key IT tools and systems should be available without being dependent on CHP infrastructure. This can be accomplished through:

- Incident tracking systems (i.e., ITSM not on local network and use of non-corporate network communication services such as 4G routers);
- Use of smart phone for all Incident Response Team Members to be used for afterhours contact and communications during incidents;
- War room as a base of operations for coordinating activities;
- Availability of laptops with mobile network modems for accessing Internet resources without relying on the internal CHP network;
- Software tool installation media kept offline and that be quickly installed on known good laptops or IT systems such as –
    - Disk copy tools;
    - Log access and analysis systems

  - Network data capture and analysis tools;
  - Forensic toolkit to analyse disk images
- Evidence gathering facilities including printers, cameras. Notebooks, chain of custody forms, evidence bags.
- Documentation for IT systems, including:
  - Asset inventory including software versions
  - Security systems, their design and security plans
  - Network diagrams
  - Logical network diagrams, including VLANS, network protocols and port;
  - Cryptographic hashes of key software and information assets for verifying their integrity.
- Known good software sources and system images for recreating information systems;
- An externally hosted emergency website for keeping staff and customers informed of incidents which can replace the normal production website through DNS changes for when the production website is unavailable;
- Internet based email service (e.g., Office 365 - Assumption that this system is no compromised);
- All Staff emergency SMS group for sending alerts where other methods are unavailable; and
- Predefined SMS Groups for coordinating activities and reporting progress.

7 Response Procedures

NOTE: If Information Technology is managed internally, please complete the following checklists. If you have an IT service provider, please request for them to complete the following checklists.

7.1 Preparation

Criteria/Trigger	Information system design and operation
Responsibility	Incident Response Team
Output	Preparedness for response to any identified security incidents
Basis/Purpose	Depending on the incident, preparation for a response to incidents could require the ability to confirm, investigate the incident, and seek the assistance of other organisations.

Task Ref.	Action / Task	Checked
01	Suitable activity logs are recorded and stored for a minimum of three months for detecting and analysing cyber security incidents	
02	All host clocks are synchronised so events can be correlated across different systems	
03	Information technology systems have adequate storage capacity to capture detailed activity logs during incidents	
04	Suitable data storage devices are available to store disk images	
05	Suitable tools are available for investigating cyber security incidents (or equivalent outsourced relationship confirmed)	
06	Tools required for incident response tasks are available offline (e.g., the tools are stored on secure removable storage devices)	
07	Staff expected to perform tasks under this plan are trained in use of supporting tools and response procedures	
08	To allow incident response teams to record network data in compliance with some state employee monitoring legislation, all information technology users are advised that all data network activity can be monitored	
09	Position descriptions and employment contracts for staff include their responsibilities for information security incident response (internal employees or contracted to CHP.)	
10	IT Administrators are authorised to take actions they deem necessary to minimise harm without prior permission	
11	An IT administrator capable of completing critical incident response activities is always available on-call and can access and manage CHP information and communication technology systems remotely	
12	A SMS group and email address has been set up to send messages to Information Security Incident response team members	
13	Suitable arrangements have been established with service providers or other organisations who are expected to support information security incident response, including:	

	• Procedures to increase the level of event logging and save critical logs (firewall, web server, VPN) for later analysis • Provide access to event logs or perform analysis of logs on demand during an incident • Provide on-call support to change configuration of devices as necessary to respond to incidents • Contact and procedures for securely exchanging sensitive data are established with • Internet Service Provider (especially for responding to Denial-of-Service attacks) • Australian Cyber Security Centre (ACSC) • Australian Federal Police • Endpoint Security software vendor • Office of the Australian Information Commissioner	

7.2 Incident Detection and Reporting

Criteria/Trigger	Information Security incident is detected
Responsibility	All staff, contractors, consultants and other users of CHP systems
Output	Initial detection report of incident
Basis/Purpose	Considerations to be made in confirming the actuality of an incident

Task Ref.	Action / Task	Checked
01	Examine automated alerts from IT systems including: • Firewall • Data Loss Prevention • Endpoint Security software • Intrusion Prevention Detection Systems • Security Event and Incident Management Systems • Mobile Device Management system • System Monitoring Software • Incident Alerts from Monitoring organisation and security intelligence organisations	
02	Analysis of event logs which should be completed on a regular basis for suspicious activity in: • Network device logs • Operating system logs • Authentication servers • Web Servers • Email servers • Application logs • Financial reconciliation systems	
03	Observations by any staff members, contractors or others. This could include: • Policy violations; • Suspicious activity • Accidental disclosure of confidential information (e.g., email sent to wrong recipient) • Loss or theft of devices or media with sensitive information • Loss of theft of building access cards • Unrecognised and unauthorised person in non-public office areas • E-mails with malicious, suspicious or misleading content • Physical tampering of IT equipment, including mobile phones, laptops and peripheral devices • Servers becoming unavailable	

	• Data inconstancies or unexplained financial reconciliation errors • Report of exploits and critical vulnerabilities • Security testing reports • Audit findings • Website defacements • Spoofed emails	
04	The person who becomes aware of an incident must report the incident to: • The Service Desk for incidents involving IT equipment, Manager for other incidents.	

7.3 Initial Triage Analysis

Criteria/Trigger	Information Security Incident reported
Responsibility	[Insert Relevant IT employees or contractor titles]
Output	Incident Record / Capture Commenced
Basis/Purpose	The person receiving an information security incident report is responsible for recording and the initial analysis of the incident

Task Ref.	Action / Task	Checked

01	**Confirm Incident**
	• Collect, store and analyse corroborative evidence as appropriate to confirm the incident. This could include:
	  ○ Identity of person reporting the incident
	  ○ Evidence of data loss or corruption (where identified or reported)
	  ○ State of production systems including network activity and CPU usage
	  ○ Email logs
	  ○ Availability of information and information systems
	  ○ Network connections on Internet firewall devices
	  ○ DHCP Logs
	  ○ Active Directory logs (regarding failed and successful logons)
	  ○ Comparison of current with baseline resource usage reports and resource usage trends
	  ○ Error logs and outages reports to exclude the possibility of human error or other known causes creating false alerts
	  ○ Internet search results for the observations
	• When assessing an incident report, the person receiving the report must be confident that the report is genuine and not a hoax or attempt to deny service for an IT system user such as having a mobile phone wiped or password disabled	

02	**Determine Scope of Incident**
	• Determine if the incident is ongoing – if so, immediate action will need to be taken to minimise harm
	• Determine the possible systems affected and if practical and time permits complete tests to determine if other systems have been affected
	• Assess the data affected by considering:
	  ○ The nature of the incident
	  ○ The systems effected
	  ○ The data available on the systems affected
	  ○ Whether personal data is at risk	

	○ If practical, assess if there is evidence of criminal activity that requires forensic evidence to be preserved. If so, note this when recording the incident and mark the incident as requiring a chain of custody for evidence collection	
03	**Rate Incident and Escalation** • Decide if immediate action is required to contain the incident. If so, act to contain the incident according to the next stage before rating the incident and creating the incident log • Rate the incident according to Table 2 above • Escalate incident according as necessary according to the rating	
04	**Create Incident Log** Create an incident log and record: • Information about the incident reported ○ The name person reporting the incident and their role, ○ Contact details of the person reporting the incident (phone numbers and email address); ○ Time the incident was reported; ○ Location of the person reporting the incident • Detail provided about the incident including: ○ Brief description of assets affected (names of workstations, servers, network device, type and brand of USB device, database, file, records as appropriate) ○ Whether privacy data is involved ○ Time of the incident or when the incident was discovered; ○ How the incident was discovered; ○ What was observed (e.g., data loss, modification, disclosure, misuse or loss of services); ○ Known details or available evidence ○ Mitigating factors (e.g., all data was encrypted, and encryption keys are safe) • Action taken to: ○ Confirm the incident ○ Investigate the scope, severity of the incident ○ Outcome of action taken • Summary of the finding ○ Summary of evidence collected ○ Functional consequences of incident (i.e., loss of information systems functionality) ○ Information impact of the incident (i.e., implications of information disclosure or modification) ○ Assigned incident severity rating if the incident is ongoing ○ If forensic evidence should be collected and the need for an evidence chain of custody	

7.4 Containment

Criteria/Trigger	Information Security Incident is confirmed	
Responsibility	[Insert Relevant IT employees or contractor titles]	
Output	Critical actions to be implemented to contain emerging incident	
Basis/Purpose	Implement actions required to contain emerging incident and prevent further damage or unauthorised access to critical systems., application and information stores	
Task	**Action / Task**	**Checked**

Ref.		
01	**Immediate response** Take action as appropriate to limit any damage and isolate affected systems from the other information systems. The general containment strategies are: • Physically isolating affected devices from other systems (for example, removing network cables and turning off wireless network, or powering down the devices); • Logically separating the devices by moving it an isolated VLAN or adding router filter or firewall rules that prevent the devices from reaching other devices or being reached from the external networks; • Removing functionality such as the software component for sending email or unmounting storage media; • Giving directions to stop data processing, e.g., if an email has been sent to the wrong recipient, advising the sender to stop sending emails, and the recipient to destroy any received emails; and • Deleting sensitive information from locations where it has been inappropriately copied or stored	
02	**Update Incident Record** Record all actions taken and include as much detail as practical. Details to include • Time • Corroborative evidence for requiring actions (e.g., data network links saturated) • Affected device(s) • Any contact with external parties to contain incident • Steps taken to contain the incident • Outcome of the action taken • Escalation of incident	

03	**Escalation and alerts**
	
	Important: If the incident analysis has identified that:
	
	• Personal Data of an identifiable individual has been breached (disclosed, corrupted, lost or deleted by an unauthorised person)
	• The PII is within the scope of the General Data Protection Regulations
	• The breach is likely to result in a risk to the rights and freedoms of individuals, including but not limited to:
	  ○ discrimination,
	  ○ damage to reputation,
	  ○ financial loss,
	  ○ loss of confidentiality or
	  ○ any other significant economic or social disadvantage
	
	Then the incident may need to be reported to clients and the individuals affected. The Incident must also be rated as critical and escalated to the Incident Response Team.
	
	Incident reports must be sent to the information system owners of the affected systems and include the current incident record.
	
	When responding to incidents, the Service Desk must escalate all Serious or Critical incidents or incidents that require alerts to be provided to other IT users, to [Insert Relevant IT employees or contractor titles] as soon as practical.
	
	When responding to incidents, the Service Desk team must escalate Serious or Critical incidents or incidents that require alerts to be sent to other staff and contractors, to the Manager as soon as practical.	

	Critical Incidents must be escalated to the Incident Response Team and Manager. Once an incident is escalated, responsibility for the incident is passed on the manager to whom the incident was escalated, and directions sought from that manager.	

7.5 Evidence Collection

Criteria/Trigger	Information Security Incident is contained and thorough investigation commences
Responsibility	[Insert Relevant IT employees or contractor titles]
Output	Incident evidence has been collected
Basis/Purpose	Implement actions required to collect and secure evidence relating to the incident

Task Ref.	Action / Task	Checked
01	While the initial analysis identifies the systems and users that are initially affected, a more thorough assessment should be performed after the containment step. This may need to include network and system administrators checking other devices such as workstations, backup storage, printers, print servers, network shares, email inbox and servers, content filtering appliances, web mail external systems and surveillance videos to confirm the extent of an incident. **Evidence to Collect** Assess the need to collect evidence of the incident and the type of evidence that would be useful. When determining the information to collect, consider: • Likely value of the information • Volatility of the information (if required volatile information should be captured as a priority) • Effort and expertise required to collect the information • Likelihood of a prosecution and the need to collect forensic evidence	
02	**Types of Evidence** Volatile data to collect (as is appropriate) in order of priority: 1 Network connections (IP addresses, network protocol and port numbers) 2 Login sessions 3 Contents of memory 4 Running processes 5 Open files 6 Network configuration 7 Operating system time 8 Network data recording network connections channels that could be used as part of an attack Non-Volatile Data to collect (as is appropriate) in order of priority: 9 For virtual servers a snapshot of the entire server should be saved before the server is shutdown. 10 For Physical servers and desktop devices - A full disk copy 11 For network-based incidents, - Increase the log levels on firewall and intrusion detection devices, web proxy or Security Incident and Event Management (SIEM) systems.	
03	**Forensic Collection Method** When collecting forensic evidence:	

	• If practical, remove and save the data media or use forensic tools that provide assurance that the data has not been modified onto a removable device
	• Store the data in a tamper evident bag, place a seal on the bag and sign the seal.
	• Document a Chain of Custody, which must record
	  ○ Identifying information for physical assets such as serial number, network device MAC addresses, brand and model number.
	  ○ A cryptographic hash of the data collected a secure hash algorithm such as SHA-256, (or enclosing a device with a signed tamper evident seal)
	  ○ The name and signature of person transferring the data
	  ○ The name and signature of the recipient / new custodian
	  ○ Date and time of the transfer
	  ○ Where the evidence is stored and how it is protected.
	• Document all steps taken to collect the information and the precautions taken to ensure the integrity of the data.
	• Verify integrity with each operation on the data
	• Cryptographic Checksums should be stored separately from the data (e.g., along with chain of custody documentation).
	
	Note: Examination, analysis and reporting should be completed by forensic experts.	

7.6 Analysis and Reporting

Criteria/Trigger	Information Security Incident is contained, and evidence has been collected
Responsibility	[Insert Relevant IT employees or contractor titles]
Output	Incident has been analysed and action plan formulated
Basis/Purpose	To fully investigate the circumstances of the incident and understand the Indicators of Compromise and systems and information affected and whether reports are required based on the information

Task Ref.	Action / Task	Checked

01	**<u>Analysis</u>**
	
	Collected evidence needs to be analysed to determine the following:
	
	• All information systems and information that any unauthorised party potentially accessed. For example, all the data on an unencrypted mobile device that was lost or stolen (this can be through an attack database that document the characteristics of known attack tools, or through analysis of recorded activity and software used in an attack);
	• Whether the information subject to the incident includes or could include personal information – if so, the information must be assessed to determine if a Notifiable Data Breach occurred – see below;
	  ○ The attack method and weakness or vulnerability exploited;
	  ○ A timeline of events;
	  ○ If any sensitive information was accessed by unauthorised persons;
	  ○ Potential consequences of the incident;
	  ○ Any residual corruption or loss in information systems resulting from the incident;
	  ○ Any other harm caused; and
	  ○ The possibility that a similar incident occurs in the future.
	
	All analysis needs to be completed on a copy of the data – not the original data or forensic copy of volatile data.	

	Recommended action to stop any incident or possible recurrences using the same or similar methods.	
02	**Notifiable Data Breach** Any incident that involves personal data must be assessed to determine if the incident constitutes a notifiable data breach. To be a notifiable data breach: 1 There is unauthorised access or unauthorised disclosure or loss of personal information that CHP holds including but not limited to: a) A staff member or contractor accesses privacy data that they are not permitted to access; b) Privacy data is sent to the wrong recipient c) Privacy data is inadvertently published in a report, website, or otherwise becomes available to unauthorised recipients d) A device or media with privacy data is lost, stolen, or not disposed of appropriately e) A cyberattack results in privacy data being read, modified or destroyed 2 It is likely (more probably than not) to result in serious harm where; a) This is considered from the perspective of a reasonable person; b) Likelihood considers the effectiveness of controls protecting the information and the potential of anyone who could possible access the information causing harm; c) Harm to the individual whose privacy data is breached considers the nature and sensitivity of the information; d) Harm can include serious physical, psychological, emotional, financial, or reputational harm including identity theft, threats to physical safety, fraud, loss of employment opportunity, bullying or marginalisation; and e) The decision need only be based on information immediately available or following reasonable inquiries or an assessment of the data breach (e.g., the personal circumstances of individuals do not need to be checked). 3 Remedial action has not been successfully taken that prevents the likelihood of serious harm (even if only to some individuals within a larger group of individuals whose information was breached). Examples of successful remedial actions include: a) Incorrect recipients of emails deleting and confirmed that the email has been deleted before it was opened; b) Wiping mobile phones that are password protected before the access could be obtained to the phone's data; and c) Disabling an authentication token before it is used by an unauthorised person; d) Removing data from a website and confirming activity logs show the data was deleted before any attempts to access the data. The assessment needs to be completed in consultation with: • The Data Owner • The Privacy Officer • Legal Counsel ***Important – if a breach of privacy is suspected, an analysis to confirm the breach needs to be completed within 30 days to comply with reporting guidelines under the notifiable Data Breaches provisions of the Australian Privacy Act. If it cannot be determined, if a breach of privacy data has occurred well within the 30days, it should be assumed that such data has been breached.***	
03	**Reporting** Important: If the incident analysis has identified a notifiable data breach, then the incident must	

	be reported to the Office of the Australian Information Commission (OAIC) and the individuals affected. The Incident must also be rated as critical and escalated to the Incident Response Team if it this is not already the case. Update the incident report with: • A summary of the evidence collected; • Evidence Analysis findings; • List of Systems and data compromised by the incident • Damaged to data and IT systems • Identity of individuals and organisations affected by the incident • Updates to the incident severity rating • Cause of the incident (if known) • Recommended next steps (for eradication) and prevention of further harm For any Serious or Critical incident, a report must be prepared for the Manager that includes the following: • A summary of the incident • Affected systems • Details of the damage caused including data that is known to have disclosed, modified or destroyed; • Whether privacy data or information belonging to an external party have been disclosed (or is more likely than not to have been disclosed) • Whether it is more likely than not that serious harm is caused because of any disclosure, corruption, loss or deletion of personal information. Important – Incident reports must be passed on in person or encrypted if using electronic communications such as email or other suitable precautions taken if the security of IT systems cannot be assured.	

7.7 Eradication

Criteria/Trigger	Information Security Incident is analysed	
Responsibility	[Insert Relevant IT employees or contractor titles]	
Output	Incident has been analysed and does not present further risk to assets and information	
Basis/Purpose	To remove software, tools and exposures within the network following containment operations	
Task Ref.	**Action / Task**	**Checked**
01	Every system compromised during an incident needs a strategy for eradicating the effects of the incident and restoring the system back to being fully operational. This should be done in collaboration with the system owner to manage outages and other risks. **Eradication Plan** Once details of an incident are known an eradication plan needs to be developed and executed that achieves the following as a minimum. • Closes any means an unauthorised party may have of accessing CHP information or IT systems. • Prevents as far as possible, unauthorised parties exploiting any authentication information (typically by changing or deactivating passwords and cryptographic keys), that could have	

	been accessed including any – ○ Passwords, including Wi-Fi passwords; ○ Password hashes; ○ Cryptographic keys, such as for private keys corresponding to public key certificates, VPN keys, Wi-Fi keys; SSH keys ○ Soft authentication tokens; ○ Wi-Fi authentication information such as WPA passwords or keys; and ○ Session authentication information stored in web cookies. Prevents as far as possible, unauthorised parties exploiting any other information that could have been accessed such as: • Changing passwords for encrypted files or for exchanging encrypted information; • Advising data owners of details of accounts that may have been exposed to prevent fraud; • Advising external parties whose data was compromised of the incident and affected data. Deletes or deactivates any executable files that could have been corrupted or shuts down IT device that could have had executable files corrupted. Verifies that only authentic and authorised programs can run on any affected network attached IT device. The resources and time required must be estimated for the eradication plan	
02	**Plan Execution** Follow emergency change management procedures to implement the eradication plan. The execution of the eradication plan should ensure that: • The resources and time to complete the eradication step are approved under emergency change management procedures • The plan is implemented correctly, and all steps are performed correctly (without errors being reported) • The plan was effective in achieving its objectives • The steps taken and outcomes of the steps are recorded in the incident record	
03	**Verification** Steps must be taken to confirm that all traces of the incident have been eradicated and the incident is no longer a risk to information systems. This includes ensuring that: • No malicious software is installed on IT systems; • All exposed passwords have been changed; • Corrupted or tampered data has been identified and will not be used; • All exposed cryptographic keys have been revoked; • Vulnerabilities used to gain unauthorised access to information systems removed or mechanisms installed to prevent the vulnerabilities being exploited; and • Disclosed confidential information has been identified and action taken to minimise harm. Should verification fail, the Evidence Collection, Analysis and Reporting and Eradication Phases need to be repeated.	
04	**Reporting** Update the incident report with: • Steps taken to eradicate the effects of the incident; • Test performed to verify effects of incident have been eradicated • Recommended next steps (further analysis or recovery)	

7.8 Recovery

Criteria/Trigger	Information Security Incident presents no further risks to assets
Responsibility	[Insert Relevant IT employees or contractor titles]
Output	Information systems have been returned to normal
Basis/Purpose	To ensure that systems and information stores are returned to conditions prior to the incident.

Task Ref.	Action / Task	Checked
01	IT systems that have been shut down, deactivated or otherwise rendered unsuitable for processing data need to be recovered so that normal data processing can be re-established. This includes: • Resetting and securing login accounts which have been compromised; • Generating and installing new cryptographic keys for any keys that were compromised; • Re-installing software that may have been compromised; • Restoring lost or corrupted data from backups; and • Reprocessing data that was possibly not processed correctly;	
02	**Strategy** Recovery strategies should follow disaster recovery plans for rebuilding systems or recovering systems from backups and know good software installation programs (e.g., from backups, original software installation media, and downloaded from authenticated vendor sites). The integrity of any data and software should be verified before being used, especially if the incident could have affected the integrity of the data. In addition to following the disaster recovery plans, special attention needs to be given to: • Using backups generated prior to date of the incident where data or software was corrupted during the incident; • Discussing options with business process owners for restoring data processed between the date of the data used for recovery and data processing that occurred since; • Replacing password data (e.g., password hashes) and cryptographic data from restored data that were changed as part of the incident response with their new valid values. • Distributing updated cryptographic data such as public key certificates, certificate revocation lists, shared cryptographic keys; • Ensuring changes to accounts are incorporated into recovered systems (that is revoked accounts are replaced with replacement accounts); and • Monitoring systems after recovery to verify that attackers do not the means to re-establish control over information systems.	
03	**Reporting** Update the incident report with: • Steps taken to recover systems (e.g., DR plan activated, and additional recovery steps performed); • Test performed to verify and confirm recovery • Recommended next steps (upgrade status of recovered systems to fully operational) to incident response team or systems owners appropriate	

7.9 Post Incident Analysis

Criteria/Trigger	Information Security Incident occurred but no longer presents a risk to assets
Responsibility	Incident Response Team
Output	Post incident report and recommendations for improvement
Basis/Purpose	To understand and communicate the lessons learnt from analysis of the incident and to improve IR operations in the future

Task Ref.	Action / Task	Checked
01	**Post Incident Analysis Objectives** The overall objectives of the post incident analysis are: • Understand the root causes that allowed the incident to occur • Determine if new or improved protective mechanisms are warranted • Assess the efficiency and effectiveness of the response in terms of the processes that worked well and where the performance could be improved • Determine if the response procedure should be changed to avoid problems that occurred or to improve the process; and • Report Recommend improvement to the executive team	

02	**Post Incident Review**
	A post incident review must be completed for all Critical incidents and for Serious incidents where the [Insert Relevant IT employees or contractor titles] determines a post incident review can be of benefit. The overall process in completing this report is as follows.
	
	• Interview key persons involved in the incident response to understand the events and seek opinions where the response work well and what they would do differently next time;
	• Determine if documented procedures were followed and if they were adequate;
	• Assess if actions should have been completed earlier or if opportunities for mitigating harm were missed;
	• Recommend any steps and tasks that can be performed differently to improve the response and costs of doing so;
	• Analyse the root causes of the incident
	• Assess the consequences of the incident and the likelihood of a similar incident occurring
	• Determine if the root cause can be addressed through actions such as:
	  ○ Changes to the incident response plan;
	  ○ Changes to standards and procedures;
	  ○ Better training;
	  ○ Improved or better use of technology;
	  ○ Better recording and analysis of events to detect incident sooner;
	  ○ Better tools for analysing and responding to incidents;
	  ○ New technical protection mechanisms for preventing vulnerabilities being exploited;
	  ○ Better incident recording and communications; and
	  ○ More authority for staff responding to incidents
	• Adjust information security risk assessment to reflect assessed consequences and likelihood of future events
	• Document findings and recommendations for the executive team to review and act upon. The report should be brief but cover the following:
	  ○ When and how was the incident was first detected, and by whom;
	  ○ Likely motivation for the attack and likely consequences of the attack;
	  ○ The scope of the incident, IT systems affected and harm to information;	

	○ Cost of the incident including consequences of the incident and costs to recover fully ○ Action taken to contain and eradicate the incident; ○ Any residual effects of incident remaining and the need for ongoing monitoring; ○ Steps taken for system recovery; ○ Areas where the response was effective; ○ Areas where the response needs improvement; ○ Underlying causes; ○ Likelihood of recurrence; ○ Recommendations to improve response; ○ Recommendations to reduce consequence and likelihood of recurrence	

Appendix A – Communications Plan

Communications are important during the whole incident response process to:

- Share information about the incident to ensure response activities are efficient;
- Keep users and stakeholder informed of incident developments and response activities; and
- Allow managers to make informed decisions.

All persons involved in the incident response are expected to convey and communicate developments and findings regularly during incident response. It is important that media statements and consistent messages about major incidents are prepared in anticipation of queries from clients, stakeholders, and the media.

The protocols, procedures, and responsibilities for communications are stated below.

External Communications

- All communications regarding information security incidents to:
  - The media,
  - CHP clients,
  - Other external parties for which CHP does not have a prior contract; must be authorised and approved by the Manager.
- All representatives of CHP communicating with the media (including social media) must be authorised to do so by the Manager
- All IT staff should be advised of an appropriate holding statement such as that they do not have any information to share about the incident at the moment and that once information is available, it will be posted on Community Housing Industry Association website
- All requests for comments or interviews with the media need to be directed to the Manager

All staff and Contractors

Staff and contractors must report information security incidents to:

- Service Desk - for any cyber security incidents (incidents involving the use of IT equipment including mobile phones and laptops, web site, emails, or remote access); and
- Immediate Supervisor or Manager - for any incident not related to IT equipment, including, incidents affecting documents, physical access cards, paper documents, intruders, and phone calls.

For current incidents (ongoing incidents) an immediate means of communications is preferred, such as a phone call. If reporting the incident using a messaging service, confirmation of receipt of the messages must be sought, for example, using the read receipt request features for email and SMS and the message must identify the best means for contacting the person reporting the incident.

Anyone reporting an incident must cooperate with the service desk team in providing as much information as they can so that the incident can be confirmed and analysed.

Service Desk Team

Where incidents are reported to the Service Desk Team, the staff member receiving the report is responsible for creating incident reports, escalating incidents when necessary and informing

system owners of incidents affecting their systems.

Service Desk Team must:

Escalate all Serious and Critical incidents or incidents that require alerts to be provided to other IT users, to the [Insert Relevant IT employees or contractor titles] as soon as practical;

- Record details of all reported incidents in incident reports listing all actions completed in analysing and handling the incident; and
- Send incident reports to the owners of the affected information systems and if requested, to the Incident Response Team

Staff must not make any statement or disclose information about information security incidents unless they have been approved for public releases. All enquiries should be referred to information on the website, or if the matter requires an urgent response to the Manager

Staff must not speculate about an incident when answering calls for information about an incident. Instead, they should assure the caller that the issue is being investigated and information will be released once CHP has investigated the incident.

[Insert Relevant IT employees or contractor titles]

The [Insert Relevant IT employees or contractor titles] must alert other internal staff or contractors as appropriate including:

- Escalating Serious incidents to the Manager
- Escalating Critical incidents to the Crisis Management Team.
- Alerting internal IT users of issues or precautions to take to prevent further incidents;
- Contacting external service providers as preapproved and required to support incident response activities including but not limited to:
  - Software and Support Vendors
  - Cloud Service provider
  - Internet Service Provider
- Forwarding details of incidents affecting cloud service to the cloud services provider for resolution;
- Keeping the Manager informed of the progress of critical incidents at least once every hour. The report should include:
  - Recent developments,
  - Actions being undertaken, and
  - Expected times for resolution of the incident

Manager

The Manager is responsible for actions including:

- Approving all statements to:
  - Law Enforcement Agencies,
  - Regulatory and statutory authorities; and
  - external organisations including for fulfilling reporting requirements under legislative, regulatory and contractual obligations
- Declaring a crisis, activating the Crisis Management Team if necessary and as advised by [Insert Relevant IT employees or contractor titles]
- Authorising reports to authorities and external parties as required
- Determining the extent of the information to be shared upon advice of the [Insert Relevant IT

employees or contractor titles], unless directed under legislation or other legal responsibility

Communications

The Manager is responsible for reviewing and approving all communications regarding an information security incident with the media and other external parties.

The Manager or delegate is also responsible for advising the most appropriate form of media for releasing information and preparing statements to the media, stakeholders and clients. Examples of possible different means of communicating with the public and includes:

- Social media (Twitter, Facebook)
- Media releases
- Press conferences
- Web site information
- Recorded messages on customer service lines
- Direct call (e.g., to affected customers)

The Manager or delegate should prepare briefings to stakeholders, alerts to send to clients and external parties whose data (including privacy data) may been disclosed to unauthorised parties.

The Manager should draft messages to staff as required to keep staff informed.

Media Training

Media training must cover the following topics:

- Only disclosing information that has been approved for public release;
- Focusing on positive aspects of disclosing information about incidents to the public fully and effectively;
- Clearly presenting CHP position and response;
- Only discussing facts and avoiding speculation;
- Protecting and keeping technical details of countermeasures secret; and
- Resisting pressure to decide on position or course of action before facts are clear and actions are authorised

Appendix B – Reporting Obligations

CHP has reporting obligations under the Notifiable Data Breaches provisions of the Privacy Act.

Privacy Data Breaches

CHP has a responsibility to ensure Notifiable Data Breaches are reported to the Office of the Australian Information Commissioner (OAIC) and affected individuals.

Notifiable Data Breaches are breaches of Personally Identifiable Information where the breach is likely to cause significant harm.

OAIC Notification

The [Insert Relevant IT employees or contractor titles], or their delegate, must with the assistance and advice of the Incident Response team determine if:

- It is likely that Privacy Data has been breached (Where privacy data is data of a personal nature where individual can be identified);
- The information can be misused to cause serious harm to the person about whom the information relates; and
- After considering the precautions and remedial actions taken, it is likely (more probable than not) that any person about whom the information related may suffer significant harm;

If after answers to the above are all affirmative, the incident must be reported to OAIC and affected individuals. Depending on the owner of the data, this may need to be done by CHP, or through the data owner themselves. Where the data owner is not CHP, this matter must be discussed with the data owner to determine the party responsible for reporting the breach.

The Manager is responsible for reporting Notifiable Data Breaches (either to OAIC and affected individuals) and must prepare the information for reporting. This must contain the following information:

- The name and contact details of the organisation reporting the breach (Community Housing Industry Association or data owner);
- A description of the eligible data breach (the incident) with sufficient information about the data breach to allow affected individuals the opportunity to properly assess the possible consequences of the data breach for them, and to take protective action in response. Suggested information includes –
  - the date, or date range, of the breach
  - the date the entity detected the data breach
  - the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure)
  - who (external party, former employee etc) has obtained or is likely to have obtained access to the information;
  - relevant information about the steps taken to contain or remediate the breach.

- The kind or kinds of information involved including whether breach involved information about an individual's –
  - racial or ethnic origin
  - political opinions
  - membership of a political association, professional or trade association or trade union
  - religious beliefs or affiliations
  - philosophical beliefs
  - sexual orientation or practices
  - criminal record
  - biometric information that is to be used for certain purposes
  - biometric templates
  - contact information (email, address, phone numbers etc)
  - other information (password hashes, test results, academic record etc)
  - financial information; and
- The recommended steps individuals at risk of serious harm take in response to the eligible data breach (refer to advice from Incident Response Team).

Important –The report must be approved by the Manager before being submitted to the data owner or OAIC

Reports to the OAIC can be completed using the OAIC reporting webpage:

https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

The report must be submitted to the OAIC within 30 days of the incident being detected, or the data owner in sufficient time for them to submit the report within 30 days of the incident being detected.

Notification to Affected Individuals

Where CHP for notifying data breaches, the Manager must prepare the notification for individuals.

Notifications can be sent through 3 different methods:

1. A notification is sent to all individuals to whom the relevant information relates. This option should be used where it is not practical to identify individuals at risk of serious harm from a breach that involves personal information about many people, but where serious harm is likely for one or more of the individuals.
2. Send a notification only to those individuals at risk of serious harm. This option is suitable when only an identified individual or known subset of individuals involved in a breach is at risk of serious harm.
3. Publish a statement on the website and take reasonable steps to publicise the contents of the statement. The statement should be available for at least 6 months. This should be used where the other options are not practical.

Notifications to individuals should be sent using their preferred method for being contacted. The notification must include information for contacting CHP about the matter.

External Party Information

Report any breaches of information belonging to an external party as required under data exchange agreement.

Other Reporting

Incidents need to be reviewed to determine if the incident should be reported to other organisations such as:

- Federal or State or Territory police or law enforcement bodies
- State or Territory Privacy and Information Commissioners
- Professional associations and professional regulatory bodies

Appendix D – Contact Details

Role	Name	Phone	Email/URL
Information Services/Service desk	[Insert Name Here]	[Insert Phone Number]	[Insert Email/URL]
IT System Administrator	[Insert Name Here]	[Insert Phone Number]	[Insert Email/URL]
Application Support & Development	[Insert Name Here]	[Insert Phone Number]	[Insert Email/URL]
Cloud services	[Insert Name Here]	[Insert Phone Number]	[Insert Email/URL]
Manager IT	[Insert Name Here]	[Insert Phone Number]	[Insert Email/URL]
Manager	[Insert Name Here]	[Insert Phone Number]	[Insert Email/URL]
Key Account Director	[Insert Name Here]	[Insert Phone Number]	[Insert Email/URL]
Communications Manager	[Insert Name Here]	[Insert Phone Number]	[Insert Email/URL]
Legal	[Insert Name Here]	[Insert Phone Number]	[Insert Email/URL]
ACSC Hotline	N/A	1300 292 371	info@cert.gov.au https://www.acsc.gov.au/incident.html
Office of the Australian Information Commissioner	N/A	1300 363 992	enquiries@oaic.gov.au https://www.oaic.gov.au
ACORN	N/A		https://report.acorn.gov.au/
State Police	[Police Station location]	[Insert Phone Number]	[Insert Email/URL]
Internet Service Provider	[Name of Provider	[Insert Phone Number]	[Insert Email/URL]