Incident Response Policy

Table of contents

Title	Incident Response Policy
Doc#	POL-SECU-010
Version	2.1
Date	28-02-2024
Supersedes	POL-SECU-010 v2.0 (19-11-2023)
Next Review	28-02-2025
Owner	Chief Information Security Officer
Approved By	Chief Executive Officer

> **POLICY INTEGRATION NOTE:** This policy should be read in conjunction with: - Business Continuity Policy POL-BC-001 (under development) - Data Breach Notification Policy POL-BREACH-001 (v1.3) - Access Control Policy POL-SECU-021 (v1.3) - Change Management Policy POL-CHANGE-001 (draft status)

CloudCore implements an information security incident response process to consistently detect, respond, and report incidents, minimise loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

The incident response process addresses:

- Continuous monitoring of threats through intrusion detection systems (IDS) and other monitoring applications;
- Establishment of an information security incident response team;
- Establishment of procedures to respond to media inquiries;
- Establishment of clear procedures for identifying, responding, assessing, analysing, and follow-up of information security incidents;
- Workforce training, education, and awareness on information security incidents and required responses; and
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders

  SCOPE LIMITATION: This policy covers information security incidents only. Physical security incidents are addressed under separate policy POL-PHYS-001 (last updated 2022 - may be outdated).

Policy Statements

CloudCore policy requires that:

(a) All computing environments and systems must be monitored in accordance to the policies and procedures specified in the following CloudCore policies and procedures:

- Auditing
- System Access

- End-user Computing and Acceptable Use

  REFERENCE ISSUE: Policy names listed above do not match current policy register: - "System Access" should be "Access Control Policy POL-SECU-021" - "Auditing" should be "System Auditing Policy POL-AUDIT-001" - "End-user Computing" policy merged into Acceptable Use Policy POL-AUP-001

(b) All alerts must be reviewed to identify security incidents.

  IMPLEMENTATION GAP: Current monitoring generates approximately 500-800 alerts daily. Policy does not specify prioritisation criteria or response timeframes for different alert types.

(c) Incident response procedures are invoked upon discovery of a valid security incident.

(d) Incident response team and management must comply with any additional requests by law enforcement in the event of criminal investigation or national security, including but not limited to warranted data requests, subpoenas, and breach notifications.

LEGAL COMPLIANCE NOTE: Australian Privacy Act 1988 requires breach notification within 72 hours. This policy does not explicitly reference Australian legal requirements.

Controls and Procedures

Security Incident Response Team (SIRT)

The Security Incident Response Team (SIRT) is responsible for:

- Review, analyse and log of all received reports and track their statuses.
- Performing investigations, creating and executing action plans, post-incident activities.
- Collaboration with law enforcement agencies.

Current members of the CloudCore SIRT:

- Security and Privacy Officer
- Security Engineers

- Head of Engineering
- DevOps and Production Support Team

TEAM COMPOSITION ISSUE: SIRT membership last updated November 2023. Several structural changes since then: - "Security and Privacy Officer" role split into two separate positions - "Head of Engineering" position vacant since January 2024 - DevOps team restructured under new "Platform Engineering" department

CONTACT DETAILS MISSING: Policy does not include 24/7 contact information for SIRT members or escalation procedures for after-hours incidents.

Incident Management Process

The CloudCore incident response process follows the process recommended by SANS, an industry leader in security. Process flows are a direct representation of the SANS process which can be found in this document.

BROKEN REFERENCE: Link to incident-flowchart.pdf returns 404 error. Document may have been moved during recent documentation system migration.

CloudCore's incident response classifies security-related events into the following categories:

- **Events** - Any observable computer security-related occurrence in a system or network with a negative consequence. Examples:

  - Hardware component failing causing service outages.
  - Software error causing service outages.
  - General network or system instability.

  CATEGORISATION ISSUE: Hardware and software failures are operational incidents, not necessarily security incidents. Classification criteria need refinement.

- **Precursors** - A sign that an incident may occur in the future. Examples:
  - Monitoring system showing unusual behaviour.
  - Audit log alerts indicated several failed login attempts.
  - Suspicious emails targeting specific CloudCore staff members with administrative access to production systems.
  - Alerts raised from a security control source based on its monitoring policy, such as
    * Okta (user authentication activities)
    * Threat Stack (AWS Cloudtrail events or system agent activities)
    * Dome9 (cloud services configuration or access alerts)
    * Carbon Black Cb Defence (malware and endpoint events)
    * Syslog events from servers

  OUTDATED TOOL REFERENCES: Several monitoring tools listed are no longer in use: - Okta replaced with Auth0 (December 2023) - Threat Stack decommissioned, replaced with Splunk (January 2024) - Dome9 replaced with Prisma Cloud (Q4 2023) - Carbon Black Cb Defence upgraded to Carbon Black Cloud (Q1 2024)

- **Indications** - A sign that an incident may have occurred or may be occurring at the present time. Examples:
  - Alerts for modified system files or unusual system accesses.
  - Antivirus alerts for infected files or devices.
  - Excessive network traffic directed at unexpected geographic locations.

- **Incidents** - A confirmed attack / indicator of compromise or a validated violation of computer security policies or acceptable use policies, often resulting in data breaches. Examples:
  - Unauthorised disclosure of sensitive data.
  - Unauthorised change or destruction of sensitive data.
  - A data breach accomplished by an internal or external entity.
  - A Denial-of-Service (DoS) attack causing a critical service to become unreachable.

CloudCore employees must report any unauthorised or suspicious activity seen on production systems or associated with related communication systems (such as email or Slack). In practice this means keeping an eye out for security events, and letting the Security team know about any observed precursors or indications as soon as they are discovered.

> **REPORTING MECHANISM GAP:** Policy states employees should "let the Security team know" but does not specify HOW - email, phone, ticketing system, or escalation procedures.

!!! Attention

```
Incidents of a severity/impact rating higher than **MINOR** shall trigger the
following response process, or as defined more specifically in the **Incident
Categories and Playbooks** section.
```

> **SEVERITY CLASSIFICATION INCONSISTENCY:** Policy references MINOR/MAJOR/CRITICAL severity levels but the classification section below uses different terminology.

I - Identification and Triage

1. Immediately upon observation CloudCore members report suspected and known Events, Precursors, Indications, and Incidents in one of the following ways:

    1. Direct report to management, the Security Officer, Privacy Officer, or other;
    2. Email;
    3. Phone call;
    4. Submit an incident report online via CloudCore Internal ServiceDesk;
    5. Secure chat; or
    6. Anonymously through workforce members desired channels.

    BROKEN LINK: ServiceDesk link is empty/non-functional.

    CONTACT INFORMATION MISSING: No specific email addresses, phone numbers, or chat channels provided for incident reporting.

2. The individual receiving the report facilitates the collection of additional information about the incident, as needed, and notifies the Security Officer (if not already done).

    ROLE AMBIGUITY: "Security Officer" role may refer to either the "Security and Privacy Officer" or new separate "Chief Information Security Officer" position.

3. The Security Officer determines if the issue is an Event, Precursor, Indication, or Incident.

1. If the issue is an event, indication, or precursor the Security Officer forwards it to the appropriate resource for resolution.
    1. Non-Technical Event (minor infringement): the Security Officer of designee creates an appropriate issue in and further investigates the incident as needed.

INCOMPLETE REFERENCE: Missing ticketing system name (likely Jira or ServiceNow).

2. Technical Event: Assign the issue to an technical resource for resolution. This resource may also be a contractor or outsourced technical resource, in the event of a lack of resource or expertise in the area.

2. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies senior leadership by email.

NOTIFICATION TIMEFRAME: No timeframe specified for senior leadership notification.

1. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
2. Once the investigation is completed, progress to Phase V, Follow-up.
3. If the issue is a technical security incident, commence to Phase II: Containment.
4. The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.
5. Each individual on the SIRT and the technical security resource document all measures taken during each phase, including the start and end times of all efforts.
6. The lead member of the SIRT team facilitates initiation of an Incident ticket in Security Project and documents all findings and details in the ticket.

SYSTEM REFERENCE MISSING: Incomplete reference to ticketing system.

* The intent of the Incident ticket is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.
* Each Incident ticket should contain sufficient details following the [SANS Security Incident Forms templates](https://www.sans.org/score/incident-fo
as appropriate.

3. The Security Officer, Privacy Officer, or CloudCore representative appointed notifies any affected Customers and Partners. If no Customers and Partners are affected, notification is at the discretion of the Security and Privacy Officer.

   NOTIFICATION INCONSISTENCY: References both singular "Privacy Officer" and combined "Security and Privacy Officer" roles.

   CUSTOMER NOTIFICATION TIMEFRAME: No timeframe specified for customer notification, which may conflict with contractual SLAs and regulatory requirements.

4. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary resources, both internal to CloudCore and potentially external.

II - Containment (Technical)

In this Phase, CloudCore's engineers and security team attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

EVIDENCE HANDLING GAP: Policy mentions evidence collection but does not reference chain of custody procedures or forensic evidence handling standards.

1. Review any information that has been collected by the Security team or any other individual investigating the security incident.
2. Secure the blast radius (i.e. a physical or logical network perimeter or access zone).

   TYPO: "access sone" should be "access zone" - indicates lack of proofreading.

3. Perform the following forensic analysis preparation, as needed:

   1. Securely connect to the affected system over a trusted connection.
   2. Retrieve any volatile data from the affected system.
   3. Determine the relative integrity and the appropriateness of backing the system up.
   4. As necessary, take a snapshot of the disk image for further forensic; and if appropriate, back up the system.

   INCOMPLETE SENTENCE: "for further forensic" - missing word (analysis/investigation).

```
5. Change the password(s) to the affected system(s).
6. Determine whether it is safe to continue operations with the affect
   system(s).
```

TYPO: "affect" should be "affected" - grammar error.

7. If it is safe, allow the system to continue to function; and move to Phase V, Post Incident Analysis and Follow-up.
8. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.
9. The individual completing this phase provides written communication to the SIRT.

COMMUNICATION METHOD: No specification of how/where written communication should be provided.

4. Complete any documentation relative to the security incident containment on the Incident ticket, using SANS IH Containment Form as a template.
5. Continuously apprise Senior Management of progress.

UPDATE FREQUENCY: "Continuously" is impractical - no specific timeframe or trigger events defined.

6. Continue to notify affected Customers and Partners with relevant updates as needed.

III - Eradication (Technical)

The Eradication Phase represents the SIRT's effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

1. Determine symptoms and cause related to the affected system(s).
2. Strengthen the defences surrounding the affected system(s), where possible (a risk assessment may be needed and can be determined by the Security Officer). This may include the following:
    1. An increase in network perimeter defences.
    2. An increase in system monitoring defences.
    3. Remediation ("fixing") any security issues within the affected system, such as removing unused services/general host hardening techniques.
3. Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.

VULNERABILITY ASSESSMENT SCOPE: No timeframe specified for vulnerability assessment completion or criteria for determining assessment scope.

1. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimise potential future compromises.

4. Update the Incident ticket with Eradication details, using SANS IH Eradication Form as a template.
5. Update the documentation with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).
6. Apprise Senior Management of the progress.
7. Continue to notify affected Customers and Partners with relevant updates as needed.
8. Move to Phase IV, Recovery.

IV - Recovery (Technical)

The Recovery Phase represents the SIRT's effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.

1. The technical team determines if the affected system(s) have been changed in any way.

    1. If they have, the technical team restores the system to its proper, intended functioning ("last known good").
    2. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).

    BUSINESS UNIT COORDINATION: No process defined for engaging business units or determining who has authority to approve system restoration.

3. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behaviour.
4. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behaviour.

    MONITORING DURATION: No timeframe specified for post-recovery monitoring.

5. Update the documentation with the detail that was determined during this phase.
6. Apprise Senior Management of progress.
7. Continue to notify affected Customers and Partners with relevant updates as needed.
8. Move to Phase V, Follow-up.

V - Post-Incident Analysis (Technical and Non-Technical)

The Follow-up phase represents the review of the security incident to look for "lessons learned" and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.

> **TIMEFRAME AMBIGUITY:** "Shortly after" and "one to two weeks" are inconsistent timeframes.

1. Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident.
2. A "lessons learned" section is written and attached to Incident ticket.
    1. Evaluate the cost and impact of the security incident to CloudCore using the documents provided by the SIRT and the technical security resource.

> **COST CALCULATION:** No methodology specified for calculating incident costs (downtime, response effort, lost revenue, etc.).

```
2. Determine what could be improved. This may include:

    * Systems and processes adjustments
    * Awareness training and documentation
    * Implementation of additional controls

3. Communicate these findings to Senior Management for approval and for
   implementation of any recommendations made post-review of the security
   incident.
4. Carry out recommendations approved by Senior Management; sufficient
   budget, time and resources should be committed to this activity.
```

> **IMPLEMENTATION TRACKING:** No process defined for tracking implementation of post-incident recommendations or measuring their effectiveness.

3. Ensure all incident related information is recorded and retained as described in CloudCore Auditing requirements and Data Retention standards.

> **RETENTION REQUIREMENTS:** References to "Auditing requirements" and "Data Retention standards" but no specific retention periods or storage requirements defined.

4. Close the security incident.

Periodic Evaluation

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding the CloudCore's expectation for them, relative to security responsibilities. The incident response plan is tested annually.

> **TESTING SPECIFICS:** "Tested annually" but no details on test methodology, scenarios, success criteria, or tabletop exercise requirements.

Incident Categories and Playbooks

- The IRT reviews and analyses on the security events on as part of its daily operations.

  TERMINOLOGY INCONSISTENCY: References "IRT" (Incident Response Team) but policy uses "SIRT" (Security Incident Response Team) elsewhere.

- Based on the initial analysis, an event may be dismissed due to false positives, normal business operations, exceptions that are already in place, permitted per policy, or duplicates. An audit trail will be kept for event dismissal.

  AUDIT TRAIL LOCATION: No specification of where dismissed event audit trail is maintained.

- A valid security event may be upgrade to a security incident. Upon which, an incident classification and severity is assigned as specified below.

  GRAMMAR ERROR: "may be upgrade" should be "may be upgraded".

- Record of the decision must be stored with details on date(s), name(s) of the person(s) conducted assessment.

  GRAMMAR ERROR: "conducted" should be "who conducted".

- A containment, eradication and recovery procedure is triggered based on the Category classification of the incident.
- In addition to the general incident management procedures previously described, one or more of the following playbooks are consulted based on the classification of a particular incident.

Classification

- **Category 1** – General Incidents, including physical security incidents

  SCOPE CONFLICT: Physical security incidents mentioned here but policy scope statement excludes physical security incidents.

- **Category 2** – Attacks on internal corporate infrastructure, including network, hardware, software
- **Category 3** – Malware
- **Category 4** – Attacks on external facing assets, such as website, web applications, web services. Including denial of service attacks.
- **Category 5** – Human targets, social engineering, phishing, etc.
- **Category 6** – Breach/leakage of critical or confidential data

  DATA CLASSIFICATION DEPENDENCY: References "critical or confidential data" but no link to Data Classification Policy for definitions.

Severity Levels:

- **Critical** – incident that involves immediate and significant interruption to business operations and/or breach of critical or confidential data
- **Major** – incident that involves immediate interruption to business operations but will not likely result in immediate data breach
- **Minor** – all other confirmed incidents

  SEVERITY CRITERIA GAPS: - No time-based SLAs for each severity level - No escalation criteria defined - "Immediate interruption" not quantified (minutes, hours?)

Response Procedures: Cat 1 – General Incident

- Prioritise handling the incident based on functional impact, informational effort, recoverability efforts and other relevant factors

  PRIORITISATION CRITERIA: "Other relevant factors" too vague - no specific criteria provided.

- Report the incident to the appropriate internal personnel and external organisations
- Acquire, preserve, secure, and document evidence

- Contain the incident
- Eradicate the incident
  - Identify and mitigate all factors that enabled the incident to occur
  - Remove any results of malicious activity
- Recover from the incident
  - Restore affected systems and business functions
  - Implement additional preventive measures

Response Procedures: Cat 2 – Internal Infrastructure Incident Response

Depending on the type of event, use the following incident response playbooks:

- Unauthorised Access
- Root Access
- Elevation of Privilege
- Improper Usage

EXTERNAL DEPENDENCY: Links to third-party playbooks may become unavailable or outdated. No internal backup playbooks maintained.

Response Procedures: Cat 3 – Malware outbreak

Depending on the agent type, follow these incident response playbooks:

- Malware
- Virus

Response Procedures: Cat 4 – External web attacks and DoS/DDoS attacks

- Mobilise the Engineering team to secure systems and ensure Business Continuity
- Conduct a thorough investigation of the incident
- Manage public relationships
- Address legal and regulatory requirements
- For a DDOS attack, follow the DDOS playbook
- Trigger BCDR if necessary

BCDR TRIGGER: References Business Continuity and Disaster Recovery (BCDR) but no cross-reference to BCDR policy or trigger criteria.

Response Procedures: Cat 5 – Social Engineering

Follow the Phishing incident response playbook

Response Procedures: Cat 6 – Data Leakage

Data Theft incident response playbook outlines the response instructions

Response Procedures: Special Cases

At least the following two special cases are considered when responding to an incident:

PHI/ePHI:

When a data breach occurs that involves unsecured PHI or ePHI, breach notifications must be performed according to HIPAA regulation requirements, including each individual impacted and as applicable, the covered entity and OCR (see Appendix for additional details).

> **REGULATORY MISMATCH:** HIPAA is US regulation. Australian organisation should reference Privacy Act 1988 and Notifiable Data Breaches scheme.
>
> **MISSING APPENDIX:** References appendix for additional details but no appendix included.

If the breach or potential breach impacts PHI/ePHI that belongs to a Covered Entity to which CloudCore is a Business Associate of, the IRT and management team will inform the Covered Entity per the timeframe and contact method established in the Business Associate Agreement or as described in §Breach Notification. HIPAA §164.410(b)

> **BROKEN LINK:** Reference to breach.md policy document that may not exist.

Criminal Activities:

In the event of an attack that involves suspected criminal activities, the IRT and management team will inform law enforcement.

> **LAW ENFORCEMENT CONTACT:** No specific procedures for contacting Australian Federal Police, state police, or ACSC (Australian Cyber Security Centre).

Insider Threat:

Members of the cross-discipline insider threat incident handling team include:

- Security and Privacy Officer,
- COO, and
- Head of Engineering as appropriate.

TEAM COMPOSITION OUTDATED: References positions that have changed since policy creation.

Emergency Operations Mode

If an incident constitutes an emergency – for example, a detected cyberattack that impacts production systems – CloudCore plans to operate in a "read-only" mode, to continue to provide customers access to their data. All write access is temporarily blocked and data upload is paused until the emergency is resolved. This is accomplished by updating the access policy in production AWS environments.

EMERGENCY CRITERIA: No specific criteria defined for what constitutes "emergency" requiring read-only mode activation.

CUSTOMER IMPACT: No notification process defined for customers affected by emergency operations mode.

In emergency operations mode, temporary access may be granted to security and/or engineering team to access the production environments to perform forensics, root cause analysis, eradication/remediation, or other necessary activities for incident recovery.

Tabletop Exercise

At least once per year, CloudCore security and engineering teams jointly performs a Red Team exercise and/or a simulated "drill" of an emergency cyberattack that results in one or more **CRITICAL** incidents. Depending on the type of exercise, the duration may range from 2-4 hours (simulated "drill") to a couple of weeks (full Red Teaming exercise).

EXERCISE SCHEDULING: No specific timeframe or scheduling requirements for annual exercises.

The exercise will follow a cyberattack playbook. It may be conducted with all internal resources or with the help of an external security consulting firm. The goal of the exercise is to ensure all parties involved receive proper training to handle an actual incident and to test out the documented procedures in order to identify gaps ahead of a real event. Senior leadership team may be invited to participate in the "drill" depending on the nature of the exercise or receive a readout of the outcome.

EXERCISE DOCUMENTATION: No requirement specified for documenting exercise results or implementing improvements identified during tabletop exercises.

Incident Tracking and Records

A record is created for each reported incident in Jira. Each incident record contains details about the incident capturing the incident attributes and progression, including the following as applicable:

> **SYSTEM SPECIFICATION:** Policy now specifies "Jira" but earlier sections have incomplete system references.

- Summary
- Description
- Impact
- Priority / Urgency
- Categorisation
- Analysis Notes and Comments
- Cause / Determination
- Outcome / Resolution
- Lessons Learned

If a more detailed post-mortem is applicable, the Security and/or DevOps team will create the write-up and link it in the incident record.

> **POST-MORTEM CRITERIA:** No criteria specified for when detailed post-mortem is required.

> **POLICY STATUS NOTICE:** This policy requires comprehensive review to address: - Outdated tool and system references - Inconsistent role definitions and team composition - Missing contact information and escalation procedures - Gaps in Australian regulatory compliance requirements - Broken cross-references and incomplete sections
>
> **COMPLIANCE RISK:** Current implementation may not meet Australian regulatory requirements for incident response and breach notification.