



# Incident Management Procedure

## Table of Contents

Overview .....	1
Incident Management Process .....	3
Territorial Incident Reporting Structure .....	3
Process Guidelines.....	4
Incident Recording Guidelines .....	4
Incident Recording Guidelines (Continued).....	5
Process Summary .....	5
Incident Management Procedure .....	6
Stage 1: Immediate Response .....	6
Stage 2: Reporting and Notifying .....	7
Stage 2: Reporting and Notifying (Continued) .....	9
Stage 3: Investigation/Incident Review .....	10
Stage 4: Action Plan and Closure .....	11
Management Reporting .....	12
Responsibility Assignment (RACI) Matrix.....	13
Accountability.....	13
Location .....	13
Feedback.....	13
Related Documents and References.....	14
Document Control Information.....	16

## Overview

<b>Overarching Policy</b>	This procedure implements and should be read in conjunction with the Incident Management Policy (GO_QA_POL_TCIM).
<b>Purpose</b>	To specify the process and key steps to effectively respond to, report and manage client incidents arising from The Salvation Army (TSA) mission delivery and enable continual improvement through systematic incident handling, reporting, analysis and change management.
<b>Who does this apply to?</b>	This procedure applies to all incidents where a client, participant, beneficiary or community member has been: <ul style="list-style-type: none"> <li>Adversely impacted in a TSA activity, program or service delivered by a mission expression</li> <li>Adversely impacting personnel or other client, participant, beneficiary or community member in a TSA activity, program or service</li> </ul>
<b>Effective date</b>	06/04/2022


## Definitions

Definitions are located in the [Glossary of Terms and Definitions](#).

Term	Definition
<b>Action Plan</b>	Specific corrective actions to be implemented in response to the identified factors/causes/findings of the incidents/feedback, who is responsible for these actions and when this is to be implemented.
<b>Affected Person</b>	The person who has been impacted or affected by an incident.
<b>Alleged Person</b>	The person who is a subject of allegation or has been accused of an incident.
<b>Breakthrough Improvement</b>	Breakthrough improvements are major improvement initiatives in key business areas with the aim of achieving significant performance improvements (ranging from 50% to 95% of baseline).
<b>Case Review</b>	A less complex process to review available information including speaking to the people involved to explore what might have caused the incident.
<b>Category 1 Incident</b>	A critical incident or alleged critical incident that has a severe impact.
<b>Category 2 Incident</b>	A critical incident or alleged critical incident that has a major impact.
<b>Category 3 Incident</b>	A non-critical incident or alleged non-critical incident that has a minor impact.
<b>Community Member</b>	Member of the public.
<b>Contributing Factors</b>	Obvious conditions and known issues that exist which cause or increase the likelihood and/or severity of an incident.
<b>Corrective Actions</b>	Any action taken to prevent reoccurrence or reduce the impact an undesirable event.
<b>Improvement Plan</b>	A plan to improve TSA's equipment, processes or systems in order to eliminate undesirable situations. Medium to long term improvements needs to be a part of a broader Continuous Improvement Plan.
<b>Incident Investigation</b>	A formal process of gathering and examination of information and evidence of an incident that requires a high level of skill to: <ol style="list-style-type: none"> <li>1. Ascertain the facts relating to an incident which may inform any subsequent criminal, civil penalty, disciplinary or administrative sanctions</li> <li>2. Substantiate an allegation</li> </ol>
<b>Incident Management System</b>	A TSA software system designed to record, manage and report on client/participant/community member/beneficiary incidents.
<b>Incident Owner</b>	The TSA person assigned ownership of the incident and who is responsible for ensuring the incident is managed in accordance with TSA policy and procedures.
<b>Incident Review</b>	The process of analysing an incident to: <ul style="list-style-type: none"> <li>▪ Identify what happened</li> <li>▪ Determine whether an incident was managed appropriately</li> <li>▪ Identify causes of the incident</li> <li>▪ Identify subsequent learnings and opportunities for improvement to reduce the risk of future harm</li> </ul> <p>There are two types of incident review:</p> <p><b>Case review</b> A less structured and resource-intensive review than a root cause analysis review to identify what happened and any process and system issues.</p> <p><b>Root cause analysis (RCA) review</b> A structured review process for identifying the true underlying cause(s) of an incident in order to facilitate learning from the incident.</p>
<b>Near Miss</b>	An incident has occurred/is occurring and a negative impact did not result due to staff intervention or a break in the chain of events or by fortune.
<b>Root Cause</b>	The underlying causes that create the existence of conditions and issues of an incident. Eliminating root causes is a robust approach to reoccurrence prevention.
<b>Root Cause Analysis (RCA)</b>	Systematic method for comprehensively analysing an incident in order to identify root causes.

# Incident Management Process

## Territorial Incident Reporting Structure

 Guidance on managing incidents that are not covered by this procedure is shown below.

---

### Child abuse related incidents

All alleged, suspected or actual child abuse, neglect, harm of risk of harm related incidents must be reported to the relevant statutory authority (i.e. police, child protection authority) as per state/territory regulations and the TSA Responding to Safeguarding Concern Procedure (GO\_LR\_PRO-01\_TPOI\_V1-0)

The relevant divisional Safeguarding Consultant must be notified of all alleged, suspected or actual child abuse, neglect, harm of risk of harm related incidents, in addition to line management notifications and statutory reporting

[Link to Workday](#) showing current Safeguarding Consultants.



Any alleged, suspected or actual child abuse, neglect, harm of risk of harm related incidents must be reported in the incident management system.

[\[Link to Incident Management System\]](#)

---

### Fraud incidents

Report according to Fraud Reporting Procedure (GO\_LR\_PRO-01\_TFRC).  
Fraud Helpline: 1800 658 966

---

### IT incidents

All IT operational and cyber security incidents must be directed to the IT Department.

ITS Helpdesk: 1300 65 00 95 or [helpdesk@aus.salvationarmy.org](mailto:helpdesk@aus.salvationarmy.org)

---

### Personnel (employees, volunteers and officers)

All incidents involving TSA personnel breaching legislation or TSA policy must be directed to the relevant HR business partner, Volunteer Resources or Officer Personnel and follow:

Employees and volunteers - Grievance Resolution Procedure (BS\_HR\_PRO-03\_TWPR).

Officers - Appropriate Workplace Behaviour Procedure - Officer to Officer Grievance (BS\_OF\_PRO-03\_TOSC).

Whistleblower Protections Policy (GO\_LR\_POL\_TWBP).

---

### Privacy incidents

Report to privacy officer as per Data Breach Response Procedure (GO\_LR\_PRO-01\_TPAC).

Privacy Officer: 1800 961 088 or email [privacy@salvationarmy.org.au](mailto:privacy@salvationarmy.org.au) or complete the Data Breach Report Form.



All privacy incidents related to clients, participants, beneficiaries, community members must be reported in the Incident Management System following notification to the Privacy Officer.

---

### WHS incidents

Report and follow WHS Hazard and Incident Reporting Procedure (GO\_WH\_PRO-13\_TWHS).

Select 'Reporting an Incident' on [Solv Safety](#) (Workplace Health and Safety System).

---

## Process Guidelines

### Accountability

Accountability for incident management will default to the Head of Department or Divisional Commander or authorised person accountable for the part of TSA in which the incident relates.

### Responsibility

All incidents must have an assigned incident owner.

The incident owner is responsible for ensuring the incident is managed in accordance with TSA policy and procedure.

In the absence of an authorised person, the Service/Site/Program/Operations manager or corps officer will be the default incident owner for the site in which the incident relates.

If an incident is incorrectly assigned, transfer of ownership of the incident must be agreed with the receiving manager (the incoming new incident owner).

## Incident Recording Guidelines

### Recording incidents

All incidents are to be recorded in the SolvSafety incident management system [\[Link to Incident Management System\]](#). Use of other IT systems to manage incidents must be approved by the Executive Manager, Continuous Improvement through your line manager.



Where required by legislation, regulation or contract, external reporting must be undertaken in addition to TSA's internal recording and reporting.

### Alternative Client Incident Management Systems

Below are alternative mission specific systems used to report and manage incidents.

- Aged Care: iCare and AlayaCare
- Salvation Army Stores: SolvSafety: Security Incidents



Guidance on system selections for specific type of incidents is documented in the Incident Systems Matrix below.

Which Internal IT System Used to Report an Incident					
Alleged Person	Affected Person	WHS Related Incidents	TSA Property related incident (exclude Salvation Army Housing property)	HR Related Incidents	Safeguarding Related Incidents
Client, participant, beneficiary, community member	TSA personnel	SolvSafety Incident Management + SolvSafety WHS	SolvSafety Incident Management + SolvSafety WHS	N/A	N/A
TSA personnel	Client, participant, beneficiary, community member	SolvSafety Incident Management + SolvSafety WHS	SolvSafety Incident Management + SolvSafety WHS	SolvSafety Incident Management	SolvSafety Incident Management
Client, participant, beneficiary, community member	Client, participant, beneficiary, community member	SolvSafety Incident Management + SolvSafety WHS	SolvSafety Incident Management + SolvSafety WHS	N/A	SolvSafety Incident Management

## Incident Recording Guidelines (Continued)

### Maintain the incident record through regular updates

All information pertaining to the management of the incident is required to be regularly updated until the incident is finalised and closed.

Incident information includes:

- Data that is entered in the system,
- Uploads of files (emails, reports, case notes, etc.)

Links to other systems of directories where files are stored

Any information that meets the criteria of personal information must meet the legislative requirements of the Privacy Act 1988.



Any information that is private or confidential in nature must not be entered into any incident management system that cannot be secured. This includes information that could put any individual at risk.

## Process Summary

The incident management process has been divided into 4 key stages:

Stage 1 Immediate Response	Stage 2 Reporting and Notifying	Stage 3 Incident Review/ Investigation	Stage 4 Action Plan and Closure
<ul style="list-style-type: none"> <li>▪ Ensure safety</li> <li>▪ Call for assistance</li> <li>▪ Activate local emergency/evacuation plan</li> <li>▪ Preserve the scene</li> <li>▪ Document facts</li> <li>▪ Manage media</li> <li>▪ Provide support</li> </ul>	<ul style="list-style-type: none"> <li>▪ External notification</li> <li>▪ Internal notification and escalation</li> <li>▪ Assign incident owner</li> <li>▪ Communicate with impacted parties</li> <li>▪ Initial review</li> </ul>	<ul style="list-style-type: none"> <li>▪ Incident review or</li> <li>▪ Investigation</li> </ul>	<ul style="list-style-type: none"> <li>▪ Develop action plan</li> <li>▪ Close incident review/investigation</li> <li>▪ Implement action plan</li> <li>▪ Close incident</li> <li>▪ Post incident review</li> </ul>

# Incident Management Procedure

## Stage 1: Immediate Response

If the incident does not require an immediate response continue directly to Stage 2 of this procedure.

---

### Ensure safety

1. If safe to do so, contain or isolate any harm so that the incident impact does not increase.
2. Implement additional actions including any restrictions to behaviour that further reduce the likelihood of harm occurring.
3. Provide first aid as required.



For child related incidents where abuse, neglect, harm or risk of harm to a child has been identified, take immediate action to ensure the safety of the child including reporting to the relevant state/territory statutory authorities. Notify the relevant divisional Safeguarding Consultant. [\[Link to Workday showing current Safeguarding Consultants\]](#).

---

### Call for assistance

1. Call for assistance from other TSA personnel as required.
2. Call external emergency services and/or crisis management team as required
3. For child related incidents where abuse, neglect, harm or risk of harm to a child has been identified and there is immediate danger to a child, call police on 000
4. Inform the relevant line manager or equivalent as soon as reasonably possible
5. Where applicable activate an existing emergency management plan.



Follow any instructions given by an authorised external party or senior TSA representative.

For Category 1, the Service/Site/Program/Operations manager or corps officer must be notified of the incident immediately by phone.

See the Incident Categorisation Notification Table (GO\_QA\_CHA-01\_TCIM) for incident categories and notification timeframes.



Incident ownership initially defaults to the relevant Site/Service/Program/Operations manager or corps officer of the location where the incident occurred.

---

### Preserve the scene

If police are called, ensure that the scene of the incident is preserved, and any physical evidence is not disturbed or taken before the police arrive.

---

### Document the facts

From the witnesses and parties involved, request the names, contact details and their account of the incident.



Reassure people that the information will be used to understand what happened.

---

### Manage Media Relations

A senior manager or above in your direct line of management is to contact Media Relations promptly if external news and media are present or aware of the incident.



Only trained and authorised Subject Matter Experts with the permission from Media Relations are allowed to respond and make public comment.



All public communication must be compliant with the Media Relations Policy (BS\_PR\_POL\_TMED) and the Code of Conduct Policy (GO\_LR\_POL\_TCOC) and Code of Conduct Standard (GO\_LR\_PRO-01\_TCOC).

---

### Provide Support

Arrange personalised support for those affected by the incident by initially ensuring a safe and secure environment and then managing any debriefing, counselling, rehabilitation or other support that may be needed in the future because of the incident.

Affected TSA personnel can access the Employee Assistance Program (EAP) for free confidential counselling sessions. Appropriate and timely follow-up counselling and support can be offered subsequently.

---

## Stage 2: Reporting and Notifying

---

**External reporting** Where required by state/territory legislation, regulation or contract, external reporting must be undertaken as a priority in addition to TSA's internal recording and reporting requirements.

Notify external parties in accordance with funding, contractual and regulatory obligations (e.g. notifiable/reportable incidents).

Where the incident relates to a child, children or young person/s, is criminal in nature and/or involves abuse, neglect, harm or risk of harm, TSA must report the incident to police and the relevant state/territory statutory and regulatory authorities, as required, without delay.



External reporting is in addition to the mandatory internal TSA reporting and notifications.

All external reports must:

- Comply with statutory and regulatory reporting obligations
- Comply with all privacy and confidentiality obligations
- Protect the integrity of any required investigations
- Be recorded in the incident management system

---

### Internal reporting 1. Internal reporting

Enter the incident details directly into the incident management system [\[Link to Incident Management System\]](#).

Where required, also complete the incident information in case notes or in relevant client management system (e.g. SAMIS). Where this is not possible, record in an alternative digital or paper-based form and arrange for entering into the incident management system in a timely manner.

All incidents are classified during the recording stage to support management of the incident and also systematic review and analysis. Refer to Incident Categorisation Notification Table (GO\_QA\_CHA-01\_TCIM) for incident classifications and categorisation.

Incident details can be entered into the incident management system by TSA personnel reporting the incident.

### 2. Assign the incident to an incident owner

The default incident owner is the Site/Service/Program/Operations manager or corps officer.



At all times an incident must have an assigned incident owner.

The incident owner is responsible for ensuring the incident is managed in accordance with TSA policy and procedure. The

Site/Service/Program/Operations manager or corps officer will be the assigned incident owner for the site in which the incident relates to in the absence of a delegated person.



For Category 1, the Site/Service/Program/Operations manager or corps officer must be notified of the incident immediately by phone. If the manager is not available, the next line of management should be notified. See the Incident Categorisation Notification Table (GO\_QA\_CHA-01\_TCIM) for incident categories and notification timeframes.

3. Ensure all digital and paper forms are stored securely in accordance with Knowledge, Information and Data Management Policy (GO\_LR\_POL\_TKID).



---

The recording of incidents must occur within the following timeframes.

Category 1 and 2 Incidents	Category 3 Incidents
Recorded as soon as reasonably practicable and no later than by the end of the work day.	Recorded within 48 hours of the incident occurring.

**Internal notification and escalation**

Initiate internal notifications in accordance with the Incident Categorisation Notification Table (GO\_QA\_CHA-01\_TCIM).



The Service/Site/Program/Operations manager or corps officer being the default incident owner, may escalate ownership of an incident according to the seriousness or category of the incident. Notification occurs via the medium most appropriate to the nature and urgency of the incident. Phone is normally the medium for urgent notification and should be backed up with an email notification.



Where the incident owner has an actual or perceived to have conflicts of interests in relation to the incident, then assign ownership to the next level manager in your line of management.

**Communicate with impacted parties**

Communicate sensitively with any injured or impacted parties or next of kin at regular intervals in the incident management process.

The principles of Open Disclosure shown below guide such communication:

- Open and timely communication
- Acknowledgement of the event
- Apology or expression of regret for the incident impact
- Supporting, and meeting the needs and expectations of the client, their family and carers
- Supporting, and meeting the needs and expectations of workers involved in the care or provision of the service or product
- Risk management and systems improvement
- Good governance and accountability
- Confidentiality

**Communicate with relevant external parties**

Communication with external authorities such as government services, service contract managers and insurance providers must address legislative, regulatory and contractual obligations.



See the Approved Authorities Matrix (GO\_LR\_PRO\_TAAP) for the authorisation to communicate with external authorities.

---



## Stage 2: Reporting and Notifying (Continued)

### Initial Review

1. Review the existing incident material to ensure the correct categorisation was applied and clarify notification requirements.
2. Reassign ownership of the incident if it falls in one of the specialist areas as outlined in the table below. For other type of incidents, change of ownership depends on the category of the incident.

Specialist Area	Action	Assigned To
Child related	Change ownership	PSQ Safeguarding
Fraud	Close in system	Internal Audit
Information Technology (IT)	Close in system	Information Technology
Personnel (employees)	Close in system	Human Resources
Personnel (volunteers)	Close in system	Volunteer Resources
Personnel (officers)	Close in system	Officer Personnel
Privacy	Change ownership	Privacy Officer
Work Health and Safety (WHS)	Close in system	Work Health and Safety (WHS)



Initial notification for the above specialist areas follows the relevant functional procedure (e.g. Fraud Reporting Procedure).

Where the incident ownership changes to another line management structure, any notifications not already done will be completed based on the new line management structure.

3. Assess the incident to determine the appropriate investigative method. The investigative method should either be incident review or incident investigation.



There are two types of incident review:

- Case Review
- or
- Root Cause Analysis (RCA) Review

Refer to the table below to determine the appropriate review action.

Case Review	RCA Review	Investigation
A less complex process to review available information including speaking to the people involved to explore what might have caused the incident	Required for highly complex incidents where there appear to be major systemic or process issues underpinning the incident, with multiple causes that warrant a more detailed analysis	Required for incidents that may inform subsequent criminal, civil penalty, civil, disciplinary or administrative sanctions especially for incidents involving allegation of abuse, unexplained injury of a client and poor quality of care

## Stage 3: Investigation/Incident Review

Proceed with the investigative method determined above in accordance with the instruction below.

---

### Case review/RCA review

1. The incident owner will assign an incident reviewer.
  2. The reviewer should prepare a plan that outlines the key activities to be undertaken prior to conduct the incident review.
  3. Incident reviewer will inform the incident owner of the outcome of the review.
  4. Incident owner will document the findings of the review in the system including any key learnings.
- 

### Incident investigation



Where required by legislation, regulation or contract, investigation must be undertaken within the required timeframe.



Where an incident has been reported to a statutory or regulatory body (i.e. police, child protection authority), any TSA investigation will only proceed with the explicit written approval and authority of that relevant statutory or regulatory body.



Any TSA investigation into the abuse, neglect, harm or risk of harm to a child, young person or adult by a member of personnel will be managed in accordance with the Safeguarding Investigations Procedure (GO\_LR\_PRO-03\_TPOI\_V1-0).



For all other incidents, the investigator could be an internal appointee who is trained and skilled in managing serious and complex investigations or an independent external investigator.

1. Initiate the investigation as soon as reasonably practicable after the incident is reported but not more than the following times:
    - Category 1: One business day
    - Category 2: Two business days
  2. The investigator informs the incident owner of the outcome of investigation and prepare investigation report.
  3. Incident owner documents all findings and update the incident management system with the outcome of the investigation.
  4. Incident owner to address any recommendations requiring follow up using an action plan (refer to Stage 4 – Action Plan).
-

## Stage 4: Action Plan and Closure

---

### Develop plan

1. Develop and document an action plan in response to the incident review or investigation outcome.
2. Assign an owner to each plan and/or task, a date by which the action is expected to be implemented and a review date.



The action plan is to include activities, actions, responsibilities, due dates and cost estimates to support approval of the proposed actions/activities. Priority should be given to quick and cost-effective actions.

---

### Communicate with relevant parties

Communicate with all parties involved and impacted in the incident taking into consideration how the plan is going to be communicated and what forms of communications will be used.

---

### Closure of the Incident Review/ Investigation

1. Ensure that:
    - Appropriate communications and notifications to the people impacted (clients, participants, beneficiaries, community members, TSA personnel and others) are completed and documented.
    - All mandatory information and required updates are completed in the incident management system.
    - Action plan is endorsed by general manager and/or head of department/National Director/Divisional Commander or authorised person and documented in the incident management system.
  2. To close the incident investigation/incident review, enter the investigation/incident review outcome and completion date with any additional information required in the incident management system.
- 

### Implement the Action Plan

1. Implement the action plan as an operational activity with regular reporting to the general manager/head of department/National Director/Divisional Commander on status progress.
  2. Update the incident management system with the outcomes of the action plan.
- 

### Closure of the Incident

To close the action plan:

- Ensure that all tasks or activities have been implemented or incorporated into an appropriate plan and updated.
  - Seek approval from relevant line manager or authorised person to close the incident for categories 1 and 2 (where relevant) only.
  - Ensure external regulatory body approval to close has been received (if applicable).
  - Update the action plan close information in the system.
- 

### Post Incident Review - Category 1 Incidents

This review should occur about three months after incident closure and at a minimum ensure:

- The incident was managed and investigated in accordance with this procedure
- All actions and plans were appropriate and effective

Reviews may be carried out internally by TSA or by external bodies.

---

# Management Reporting

---

## Review a monthly report

State/General Managers/Executive Managers/Area Officers generate a monthly report from the incident management system covering their area of responsibility and review:

- The number of open incidents
- The status of any improvement plans
- The effectiveness of improvement actions

Follow-up conversations are required where there is a concern:

- In trends of incidents
  - Excessive delays in the management of incidents
- 

## Review a quarterly report

Heads of department, National Directors and Divisional Commanders should generate a quarterly report from the incident management system covering their area of responsibility and review trends and the effectiveness of improvement plan implementation.

---

## High-level data analysis framework

Incident data analysis includes the monitoring, interrogating and acting on trends identified through the analysis of incident information.

The purpose of data analysis is intended to:

- Learn from patterns and trends of client incidents
  - Ongoing identification of issues and implementation of changes that result in improved services and better outcomes for client safety and wellbeing
  - Strategic prioritisation and resourcing
  - Good governance of quality performance and continuous improvement activities
-

# Responsibility Assignment (RACI) Matrix

The roles associated with execution of this procedure are indicated in the table below.

Stage	Activity	TP	LM	IO	SR	INV/ INR	GM/ EM/AO	HoD/ ND/ DC
1.	Immediate Response	R	A					
2.	Reporting and Notifying			R	I			A
3.	Investigation/Incident Review				I	R		A
4.	Action Plans and Closure			R	I			A
	Management reporting				R		R	A

**Legend:**

R – Responsible, A – Accountable, C – Consulted, I – Informed

TP – TSA Personnel, LM – Line Manager, IO - Incident Owner, SR - Senior TSA Representative,

INV – Investigator, INR – Incident Reviewer, GM/EM/AO General Manager/Executive Manager/Area Officer, HoD - Head of Department, ND – National Director, DC – Divisional Commander

## Accountability

**Obligation**

All TSA personnel under the terms of their service, employment, engagement or contract must comply with all TSA policies, procedures and supporting documents.

**Consequences of non-compliance**

Failure to comply with this procedure may result in disciplinary action and, in serious cases, termination of employment or engagement with TSA.

## Location

**Repository**

Territorial Policy Hub

## Feedback

**Feedback is encouraged**

Feedback is used to improve and enhance the impact of this procedure. It will be considered when reviewing and updating the document.

**Who is feedback provided to?**

All feedback is to be forwarded to [continuousimprovementthq@salvationarmy.org.au](mailto:continuousimprovementthq@salvationarmy.org.au).

## Related Documents and References

---

**Policy Documents**

Incident Management Policy (GO\_QA\_POL\_TCIM)

Procedures

Incident Management Procedure (GO\_QA\_PRO-01\_TCIM)

Charts

Incident Categorisation Notification Table (GO\_QA\_CHA-01\_TCIM)

Incident Management Process Chart (GO\_QA\_CHA-02\_TCIM)

Guides

SolvSafety User Guide - Report an Incident (GO\_QA\_GUI-01\_TCIM)

SolvSafety User Guide - Manage an Incident (GO\_QA\_GUI-02\_TCIM)

Incident Investigation Guidelines (GO\_QA\_GUI-03\_TCIM) to be developed

Forms

Incident Report Form (GO\_QA\_FOR-01\_TCIM)

Investigation Action Plan Template (GO\_QA\_FOR\_02\_TCIM)

RCA Tool - Cause and Effect Diagram Template (GO\_QA\_FOR\_03\_TCIM)

RCA Tool - Five Why Diagram Template (GO\_QA\_FOR\_04\_TCIM)

Root Cause Analysis Action Plan Template (GO\_QA\_FOR\_05\_TCIM)

Root Cause Analysis Review Template (GO\_QA\_FOR\_06\_TCIM)

Case Review Action Plan Template (GO\_QA\_FOR\_07\_TCIM)

Case Review Template (GO\_QA\_FOR\_08\_TCIM)

---

**Related Policy Documents**

Appropriate Workplace Behaviour Procedure - Officer to Officer Grievance (BS\_OF\_PRO-03\_TOSC)

Approved Authorities Matrix (GO\_LR\_PRO\_TAAP)

Code of Conduct Policy (GO\_LR\_POL\_TCOC)

Code of Conduct Standard (GO\_LR\_PRO-01\_TCOC)

Compliance Policy (GO\_LR\_POL\_TCOM)

Data Breach Response Procedure (GO\_LR\_PRO-01\_TPAC)

Enterprise Risk Management Policy (GO\_LR\_POL\_TERM)

Feedback and Complaints Policy (GO\_LR\_POL\_TFBK)

Fraud Policy (GO\_LR\_POL\_TFRC)

Fraud Reporting Procedure (GO\_LR\_PRO-01\_TFRC)

Governance Policy (GO\_LR\_POL\_TGOV)

Grievance Resolution Procedure (BS\_HR\_PRO-03\_TWPR)

Knowledge, Information and Data Management Policy (GO\_LR\_POL\_TKID)

Media Relations Policy (BS\_PR\_POL\_TMED)

Person of Interest (Safeguarding) Policy (GO\_LR\_POL\_TPOI)

Quality Management Policy (GO\_QA\_POL\_TQCI)

Responding to Safeguarding Concerns Procedure (GO\_LR\_PRO-01\_TPOI)

Safeguarding Investigations Procedure (GO\_LR\_PRO-03\_TPOI)

Safety and Wellbeing of Children and Young People Policy (GO\_LR\_POL\_TSWC)

Whistleblower Protections Policy (GO\_LR\_POL\_TWBP)

Work Health and Safety Policy (GO\_WH\_POL\_TWHS)

WHS Hazard and Incident Reporting Procedure (GO\_WH\_PRO-13\_TWHS)

Links to Systems used by TSA

[Incident Management System](#)

[Solv Safety](#)

[Workday](#)

---



<b>Related Legislation</b>	Care and Protection of Children Act 2007 (NT) Children and Young People Act 2008 (ACT) Children and Young Persons (Care and Protection) Act 1998 (NSW) Children, Young Persons and their Families Act 1997 (Tas) Children, Youth and Families Act 2005 (Vic) Children Legislation Amendment (Reportable Conduct) Act 2017 Children and Community Services Act 2004 (WA) Children's Protection Law Reform (Transitional Arrangement and Related Amendments) Act 2017 (SA) Children's Protection Act 1993 (SA) Child Wellbeing and Safety Amendment (Child Safe Standards) Act (Vic) 2015 Child Safety (Prohibited Persons) Act 2016 (SA) Child Safety (Prohibited Persons) Regulations 2016 (SA) Child Protection Act 1999 (Qld) Commissioner for Children and Young People Act 2006 Criminal Records Act 1991 (NSW) Crimes Act 1914 (Cth) Domestic and Family Violence Act 2007 (NT) Ombudsman Act 1974 Part 3A (NSW) Privacy Act 1988 (Cth) Reportable Conduct and Information Sharing Legislation Amendment Act 2016 Victorian Crimes Act 1958 (Vic) (Section 49B, 49C, 327)
<b>Funding Agreement Requirements</b>	NA
<b>Governance/ Accreditation/ Certification Standards</b>	NA
<b>Audit Report Findings</b>	NA
<b>Other Relevant Documents /Resources</b>	Williams, R. (2008) Cultural safety; what does it mean for our work practice? <i>Australian and New Zealand Journal of Public Health</i> , 23(2), 213-214.

## Document Control Information

<b>Document ID</b>	GO_QA_PRO-01_TCIM
<b>Theme</b>	Governance
<b>Category</b>	Quality Assurance
<b>Policy Owner</b>	Assistant to the Chief Secretary – Governance Portfolio
<b>Policy Implementer</b>	Head of Quality and Safeguarding
<b>Approval Authority</b>	Australia Territory Board
<b>Review Date</b>	February 2022
<b>Next Review Date</b>	October 2023
<b>Previous Documents</b>	<b>AUE</b> Process 08 – Critical Incident <b>AUS</b> CIM Attach 01 – Critical Incident Management Procedure CIM Attach 02 – Critical Incident Categorisation Schedule CIM Attach 03 – Critical Incident Form

**Document History**

<b>Version</b>	<b>Date Approved</b>	<b>Summary of Changes</b>
1-0	07/08/2020	Inaugural version
1-1	4/04/20225	Updates to meet SA Dept of Human Services safeguarding requirements