



# Critical Incident Management Policy and Procedures

## Scope & Purpose

This policy and procedure applies to members of the Russo Business School higher education community.

The Critical Incident Management Policy encompasses the management of critical incidents. It details the arrangements that apply to critical incident management in the context of the Russo Business Schools Risk Management Framework.

This policy has been implemented to ensure an effective and timely response to a critical incident. Ensure accessibility to assistance, provide information on how to report a critical incident and provide a framework within which Russo Business School can address the immediate and possible longer term needs of those involved.

## Definitions and Abbreviations

A **critical incident** is a tragic and/or traumatic event which causes or is likely to cause extreme physical and/or emotional distress to staff and/or students and may be regarded as outside the normal range of experience of the people affected. The event has the potential to cause unusually strong emotional reactions in the Russo Business School community.

**Emergency Critical Incident** means those incidents which involve the possibility of immediate or imminent threat, physical and/or emotional distress to staff, job seekers, students and other visitors to our organisation; and which may be regarded as outside the normal range of experience of the people affected.

**Non emergency Critical Incident** means those critical incidents which do not involve the need for an initial emergency response but which nevertheless involve the possibility of threat, physical and/or emotional distress to staff, students, clients and other visitors to our organisation; and which may be regarded as outside the normal range of experience of the people affected.

Some examples of critical incidents include:

### IT System security event:

- Privacy Breach
- Cyber security breach
- Disruption events for longer than 4 hours, impacting on ability to deliver services

### Organisational Brand Management

- Negative Press
- Liable and Slander
- Defamation of character

### Personal security event:

- Fatality/near fatality
- Serious accidents murder suicide
- Threats to personal safety or abuse incidents
- Sexual assaults
- Missing student
- Threat of infectious disease (risk of an epidemic/pandemic)

### Physical/infrastructure security event:

- Fire, explosion, bomb/arson threats
- Electrical hazard, Gas leak Suspect items
- Building defects

**Legislative compliance breach**

- Statutory and regulatory
- Discrimination/Harassment
- Ethics/Integrity
- WHS
- Financial

**Natural Disasters:**

- Flood/Cyclone/Storm
- Bushfire

Every critical incident is unique and will need to be dealt with differently, according to the needs of the people affected.

**CRICOS** – Commonwealth Register of Institutions and Courses for Overseas Students

**DHA** – Department of Home Affairs

**ESOS** - Education Services for Overseas Students

**PRISMS** – Provider Registration and International Student Management System

Russo Business School (RBS) recognises that incidents can arise that have the potential to impact seriously on the safety of; staff, students, clients, contractors, volunteers and visitors on campus and/or work locations, and/or business continuity.

RBS further recognises that effective planning, management and coordination is required to ensure incidents don't become critical through inaction.

An incident may be triggered by internal or external issues such as public safety, health concerns, major fraud, breach, mismanagement or controversial academic activities. Routine or seemingly harmless activities may develop into a Critical Incident after attracting the attention of government, regulators, interest groups, the public or the media. In addition, a simple emergency or minor issue may be turned into a Critical Incident by being insensitively or poorly managed.

This policy and related entity procedures are designed to ensure the RBS Community:

- Meets its duty of care obligations in providing the highest possible standard of health and safety for staff, students, clients, contractors and visitors and other persons working at or visiting the Group's offices;
- Is able to respond swiftly and effectively in the event of a critical incident;
- Is able to respond swiftly and effectively when dealing with challenging students, clients and jobseekers;
- Implements an integrated approach to management of risks associated with incidents or critical incidents; and
- Is compliant with relevant Legislation and Standards so that:
  - Exposure of persons to health and safety risks arising from incidents or critical incidents is avoided or minimised; and
  - Physical and psychological trauma are reduced.
- Has mechanisms in place to communicate to the relevant parties and across the organisation in times of a critical incident.

The Sarina Russo Group will have processes in place to ensure that;

- Threats and potential critical incidents are regularly identified and assessed in order to strengthen the preparedness for any such events;
- Has appropriate plans in place for managing an incident;
- Has appropriate plans in place for dealing with challenging students, clients and jobseekers; and  
Can recover promptly from any crisis and resume normal business as soon as possible.

The action required following an incident will depend on its nature and severity. Even seemingly minor incidents can cause emotional and psychological trauma which may not be immediately evident.

### **Emergency Critical Incident Coordinating Team**

The Russo Business School Emergency Critical Incident Coordinating Team will be responsible for managing, coordinating, planning and implementing a timely and effective response to an emergency critical incident. This team comprises the following staff members:

- Chief Executive Officer
- Russo Business School Dean, Academic Operations
- Senior Manager, Operations
- TSRG Legal Contract Compliance Executive
- Manager, Academic Operations and Standards

The Emergency Critical Incident Coordinating Team may co-opt additional staff members or external bodies as appropriate to a particular incident.

The Legal Contract Compliance Executive from the Sarina Russo Group will act as secretariat for all Emergency Critical Incident Coordinating Team meetings.

The Emergency Critical Incident Coordinating Team will meet within one month after an emergency critical incident to evaluate the implementation of procedures and responses, and suggest improvement activities if necessary.

### ***International students***

For Internal students the following external bodies may need to be contacted:

- Department of Home Affairs
- Relevant consulate or embassy
- Overseas Health Fund Provider

### **Oversight and Evaluation**

The Manager, Academic Operations and Standards will provide regular reports to the RBS Board of Directors and the Risk Management and Compliance Committee (RMCC) in relation to critical incidents that have occurred (critical incidents are to be recorded in the RBS Critical Incident Register, including the actions implemented by the RBS managers and Emergency Critical Incident Coordinating Team where relevant) and the corresponding outcomes.

## **Procedures**

This policy outlines the procedures to be followed in the event of a critical incident involving any member of the Russo Business School (RBS) community. It has been written to assist staff and students to report and respond appropriately to incidents that are likely to cause trauma to individuals and/or affect the RBS community as a whole.

The following table shows examples of the intensity levels of a critical incident as well as brief notes on the level of reporting and follow up action required.

| Incident level   | Critical Incident types or category   | Reporting Process   | Debrief for SRG staff involved  |
|------------------|---|---|---|
|                  | <b>IT System security event:</b> <ul style="list-style-type: none"> <li>• Cyber security breach</li> <li>• Disruption events for longer than 4 hours, impacting on ability to deliver services</li> </ul>   | Notify the Chief Information Officer and Chief Information Security Officer to identify risk and remove threat.   | CIO and CISO undertake security risk assessment and corrective actions  |
|                  | <b>Privacy Breach</b> <ul style="list-style-type: none"> <li>• Personal Information is lost, subject to unauthorised access/ disclosure</li> </ul>  | Notify the Privacy Manager and General Legal Counsel of the time and date of the suspected breach, type of information involved, the cause, extent and context of the affected information. The Privacy Manager will determine whether a data breach has occurred and alert the data breach response team if required.  | Investigate cause, make appropriate changes to policies and procedures, and undertake staff training if necessary.  |
| <b>Emergency</b> | <b>Personal security event:</b> <ul style="list-style-type: none"> <li>• Fatality/near fatality</li> <li>• Serious accidents – including homicide, self-harm or harm to others</li> <li>• Threats to personal safety or abuse incidents</li> <li>• Sexual assaults</li> <li>• Missing student</li> <li>• Threat of infectious disease (risk of an epidemic/pandemic)</li> <li>• Serious student or staff misconduct</li> <li>• Drug or alcohol abuse impacting academic performance or conduct</li> </ul> | <ol style="list-style-type: none"> <li>1) <b>For all Incidents requiring an emergency service; (fire, ambulance or police) contact 000 immediately.</b></li> <li>2) The staff member who is notified or is aware of the incident must: <ol style="list-style-type: none"> <li>a) Ensure the emergency services are contacted as appropriate.</li> <li>b) immediately notify the Chief Executive Officer and/or the Emergency Critical Incident Coordinating Team (ECICT) members. Should the incident occur out of hours then the designated person must be contacted;</li> <li>c) The Chief Executive Officer and/or the ECICT must assess whether the incident is an emergency or a non-emergency critical incident.</li> <li>d) building evacuation procedures enacted controlled by the Chief Fire Warden, if appropriate;</li> <li>e) submit an incident report to <a href="mailto:incident2@sarinarusso.com.au">incident2@sarinarusso.com.au</a>; and</li> <li>f) if appropriate, record the incident on client's file</li> </ol> </li> <li>3) Should a student become aware of a Critical Incident or requires assistance they should immediately contact a staff member as listed on the <b>Sarina Russo Group Contact Card</b>.</li> <li>4) The Chief Executive Officer; the members of the ECICT; and/or the out-of-hours contact will notify; third parties as appropriate ie Managing Director, General Legal Counsel</li> <li>5) The Chief Executive Officer will convene an ECICT meeting as soon as practicable.</li> <li>6) If required, Emergency Business Continuity Plan will be enacted by the ECICT</li> <li>7) The Risk Manager must update the Critical Incident Register and include incident in a report to the RMCC at the next meeting following the incident..</li> </ol> | <ul style="list-style-type: none"> <li>• Formal team debrief</li> <li>• One on one with Manager</li> <li>• One on one with those involved as appropriate</li> <li>• Consider Employee Assistance Program</li> <li>• Review policy and procedure as appropriate</li> </ul> |

| Incident level | Critical Incident types or category   | Reporting Process  | Debrief for SRG staff involved  |
|----------------|---|--|---|
|                | <p><b>Physical/infrastructure / security event:</b></p> <ul style="list-style-type: none"> <li>• Fire, explosion, bomb/arson threats</li> <li>• Electrical hazard, Gas leak Suspect items</li> <li>• Building defects</li> </ul> <p><b>Natural Disasters:</b></p> <ul style="list-style-type: none"> <li>• Flood,,Cyclone/Storm</li> <li>• Bushfire</li> </ul>  | <p><b>1) For all Incidents requiring an emergency service; (fire, ambulance or police) contact 000 immediately.</b></p> <p>2) The staff member who is notified or is aware of the incident must:</p> <ol style="list-style-type: none"> <li>a) Ensure the emergency services are contacted as appropriate.</li> <li>b) immediately notify the Chief Executive Officer and/or the Emergency Critical Incident Coordinating Team (ECICT) members. Should the incident occur out of hours then the designated person must be contacted;</li> <li>c) The Chief Executive Officer and/or the ECICT must assess whether the incident is an emergency or a non-emergency critical incident.</li> <li>d) building evacuation procedures enacted controlled by the Chief Fire Warden, if appropriate;</li> <li>e) submit an incident report to <a href="mailto:incident2@sarinarusso.com.au">incident2@sarinarusso.com.au</a>; and</li> <li>f) if appropriate, record the incident on client's file</li> </ol> <p>3) Should a student become aware of a Critical Incident or requires assistance they can report this to the Chief Fire Warden, their Lecturer, Student Services, or The Resource Centre when on Campus</p> <p>4) The Chief Executive Officer; the members of the ECICT; and/or the out-of-hours contact will notify; third parties as appropriate ie Managing Director, General Legal Counsel, Property Manager</p> <p>5) The Chief Executive Officer will convene an ECICT meeting as soon as practicable.</p> <p>6) If required, Emergency Business Continuity Plan will be enacted by the ECICT.</p> <p>7) The Risk Manager must update the Critical Incident Register and include incident in a report to the RMCC at the next meeting following the incident.</p> | <ul style="list-style-type: none"> <li>• Formal team debrief</li> <li>• One on one with Manager</li> <li>• One on one with those involved as appropriate</li> <li>• Consider Employee Assistance Program</li> <li>• Review policy and procedure as appropriate</li> </ul> |
|                | <p><b>Organisational Brand Management</b></p> <ul style="list-style-type: none"> <li>• Negative Press</li> <li>• Liable and Slander</li> <li>• Defamation of character</li> </ul> <p><b>Legislative compliance breach</b></p> <ul style="list-style-type: none"> <li>• Statutory and regulatory</li> <li>• Discrimination / Harassment</li> <li>• Ethics/Integrity</li> <li>• WHS</li> <li>• Financial</li> </ul> | <p>The staff member who is notified or is aware of the incident must immediately notify the Chief Executive Officer and/or the General Legal Counsel.</p> <p>Should a student become aware of an they can report this to their Lecturer, Student Services, or The Resource Centre when on Campus.</p> <p>The risk will be assessed and procedures to contain/report and mitigate will be enacted.</p>  |   |

| Incident level       | Critical Incident types or category   | Reporting Process  | Debrief for SRG staff involved  |
|----------------------|---|--|---|
| <b>Non-emergency</b> | <p>Theft or vandalism (but client, staff or person was unharmed)</p> <p>Distressing or disturbing behavior (but no immediate risk to safety or wellbeing of students or staff)</p> <p>Acute but not life- threatening illness (except where there is a risk of an epidemic)</p> <p>Smells</p> | <p>1) The staff member who is notified or is aware of the incident must:</p> <ol style="list-style-type: none"> <li>a. Confirm that the incident is a non-emergency and that the emergency services are not required.</li> <li>b. Immediately notify the respective office manager/supervisor;</li> <li>c. Submit an incident report to <a href="mailto:incident2@sarinarusso.com.au">incident2@sarinarusso.com.au</a>; and</li> <li>d. If appropriate, record the incident on client's file.</li> <li>e. The Chief Executive Officer must assess whether the incident is an emergency or a non-emergency critical incident. If the incident is assessed as an emergency then the emergency critical incident procedure (see above) will apply.</li> <li>f. The Chief Executive Officer will notify the police, other offices and third parties as required.</li> <li>g. The Risk Manager must update the Critical Incident Register and include incident in a report to the RMCC at the next meeting following the incident.</li> </ol> | <ul style="list-style-type: none"> <li>• Formal team debrief</li> <li>• One on one with Manager</li> <li>• One on one with those involved as appropriate</li> <li>• Consider Employee Assistance Program</li> <li>• Review policy and procedure as appropriate</li> </ul> |





## Related legislation and standards to be read in conjunction with

[Commonwealth Register of Institutions and Courses for Overseas Students \(CRICOS\)](#)  
[Disability Standards for Education 2005 \(Cth\)](#)  
[Disaster Management Act 2003](#)  
[Educational Services for Overseas Students Act 2000 \(ESOS Act\)](#)  
[Higher Education Standards Framework \(Threshold Standards\) 2021](#)  
[Information Privacy Act 2019 \(QLD\)](#)  
[National Code of Practice for Providers of education and Training to Overseas Students 2018](#)  
[Privacy Act 1988](#)  
[Queensland Fire Regulations](#)

## Related documents

### **Policies**

*Sexual Assault and Sexual Harassment Policy and Procedure*  
*Privacy Policy*

## Delegation

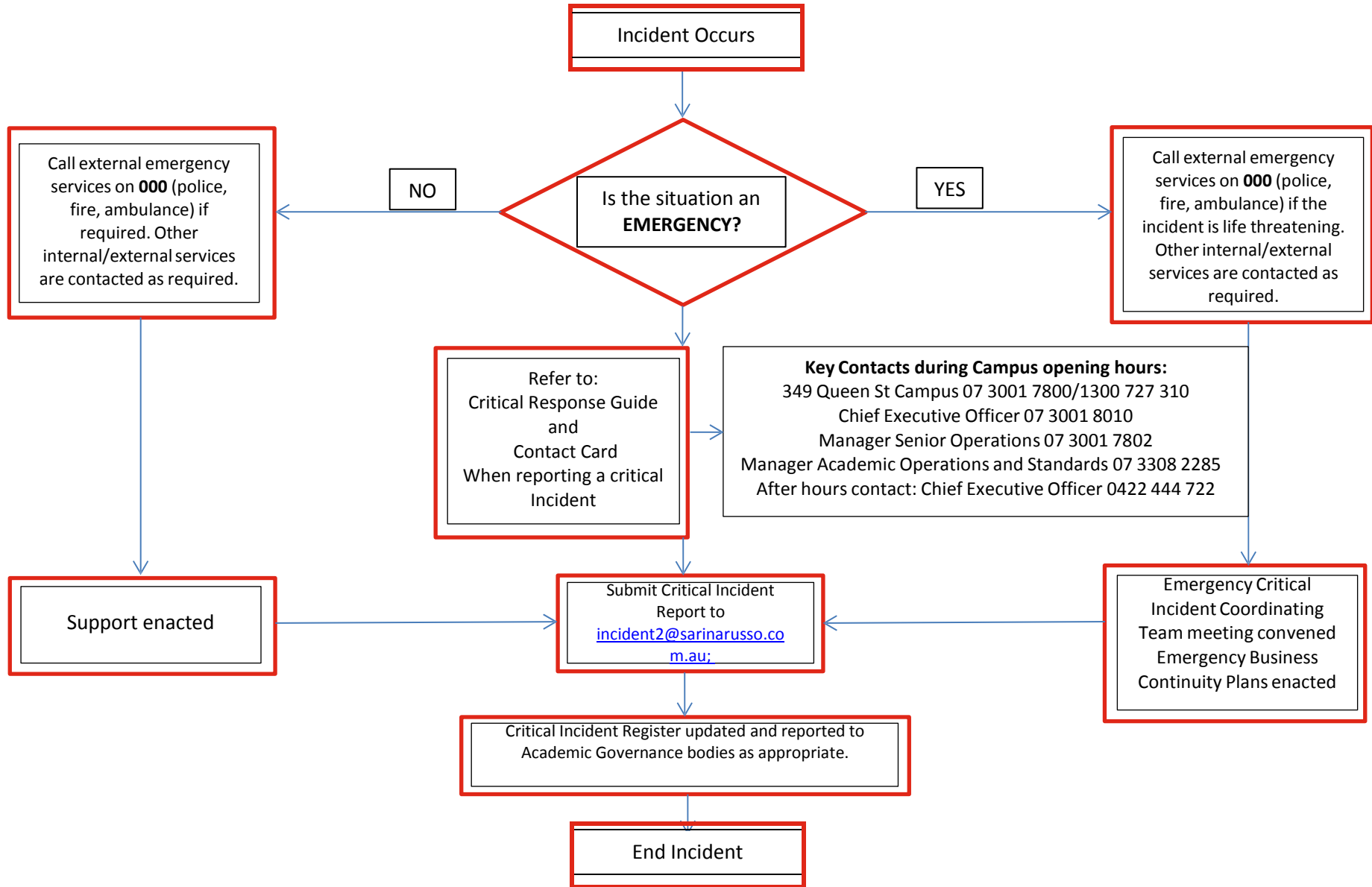
| Delegated Authority                      | Delegation   |
|--|--|
| <b>Governance</b>                        |  |
| Risk Management and Compliance Committee | Refer to Service Level Agreement Sarina Russo Job Access (Australia) Pty Ltd and Russo Business School |
| Board of Directors                       | Refer to the Terms of Reference  |
| <b>Executives</b>                        |  |
| Chief Executive Officer                  | Relevant to Accountability Statement   |

## Version control

| Policy & Procedure Version No | Policy & Procedure Sponsor               | Approval Authority                       | Date of Approval | Date for next review |
|-------------------------------|--|--|------------------|----------------------|
| 1/2017                        | Risk Management and Compliance Committee | Risk Management and Compliance Committee | 7 November 2017  | 6 April 2018         |
| 2/2018                        | Risk Management and Compliance Committee | Risk Management and Compliance Committee | 3/04/2018        | 3/04/2019            |
| 3/2020                        | Risk Management and Compliance Committee | Risk Management and Compliance Committee | 3/6/2020         | 3/6/2021             |

|        |  |  |            |            |
|--------|--|--|------------|------------|
| 4/2022 | Risk Management and Compliance Committee | Risk Management and Compliance Committee (minor amendment)             | 14/06/2022 | 14/06/2024 |
| 5/2023 | Risk Management and Compliance Committee | RBS Board of Directors Risk Management and Compliance Committee (minor | 17/03/2023 | 17/03/2025 |

Russo Business School Critical Incident Policy - Response Flowchart





Critical Incident Contact Card

**Front of Card**  
**Sarina Russo Group**  
**CRITICAL INCIDENT CONTACT CARD**

**Life Threatening?** → **0 0 0**

Your  
Manager/Lecturer  
(if not contactable)

↓

Kathleen 0422 444 722  
Newcombe  
(if not contactable)

↓

Kevin Anderson 0409 348 544  
(if not contactable)

↓

Stephanie Hunter 0400 367 051  
(if not contactable)

↓

Quentin Underhill 0429 800 814  
(if not contactable)

↓

Justin Sharp 0419 709 185  
(if not contactable)

↓

David Ormesher 0428 038 190

**ONCE YOU HAVE CONTACTED ONE OF THE  
ABOVE STAFF, THEY WILL ESCALATE THE ISSUE  
AND KEEP IN CONTACT WITH YOU**

**Main Campus:**  
1300 727 310  
07 3001 7800

**Back of card**  
**Sarina Russo Group**  
**CRITICAL INCIDENT CONTACT CARD**

**EMERGENCY 0 0 0**

**Police Link 131 444**

**ONCE YOU HAVE CONTACTED A MANAGER,  
THEY WILL ESCALATE THE ISSUE AND KEEP IN  
CONTACT WITH YOU**

**KEEP A WRITTEN RECORD OF EVENTS, TIMES  
& CONVERSATIONS**

**STAY CALM & REMAIN CONTACTABLE**

**DON'T PUT YOURSELF IN DANGER**

