

Critical Incident Management Policy

Scope & Purpose

This policy and procedure applies to all staff and students of Russo Business School Pty Ltd ABN 34 601 105 319 trading as Russo Business School (RBS) (CRICOS Provider Code – 03441F). Russo Business School is part of the Sarina Russo Group of companies.

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 such an incident and to provide a framework within which SRG can address the immediate and possible longer term needs of those involved.

Definitions and Abbreviations

DHA – Department of Home Affairs

DET – Department of Education and Training

OSHC – Overseas Health Cover Provider

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, 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.

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)

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.

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.

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
- Associate Dean, Diploma Programs
- 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 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

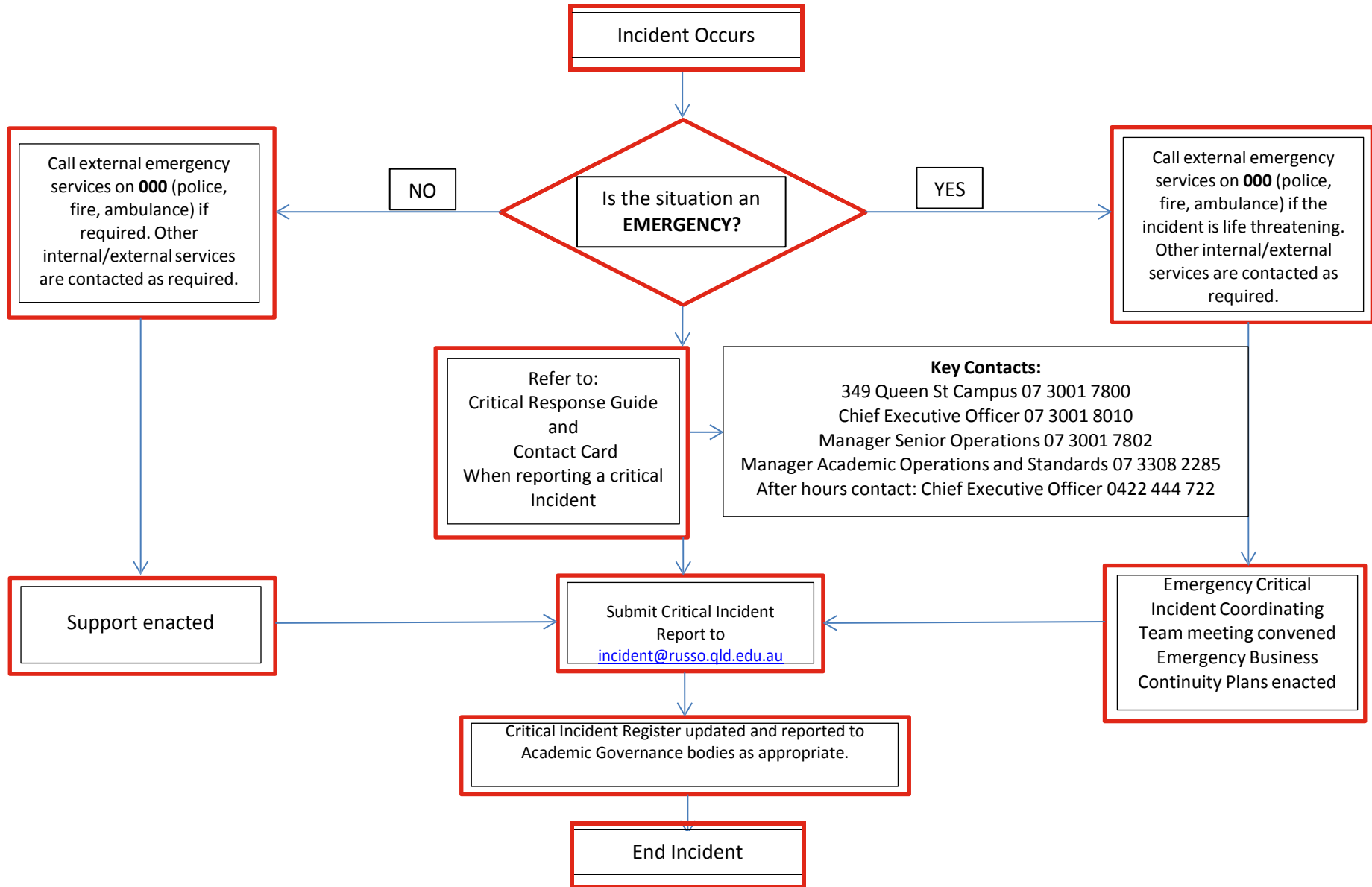
Oversight and Evaluation

The Manager, Academic Operations and Standards will provide regular reports to the RBS Board of Directors and the Audit Risk and Compliance Committee (ARCC) 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.

Critical Incident Management Policy

Incident level	Critical Incident types or category	Reporting Process	Debrief for SRG staff involved
Emergency	<p>IT System security event:</p> <ul style="list-style-type: none"> • Privacy Breach • Cyber security breach • Disruption events for longer than 4 hours, impacting on ability to deliver services <p>Organisational Brand Management</p> <ul style="list-style-type: none"> • Negative Press • Liable and Slander • Defamation of character <p>Personal security event:</p> <ul style="list-style-type: none"> • 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) <p>Physical/infrastructure security event:</p> <ul style="list-style-type: none"> • Fire, explosion, bomb/arson threats • Electrical hazard, Gas leak • Suspect items • Building defects <p>Legislative compliance breach</p> <ul style="list-style-type: none"> • Statutory and regulatory • Discrimination/Harassment • Ethics/Integrity • WHS • Financial <p>Natural Disasters:</p> <ul style="list-style-type: none"> • Flood,/Cyclone/Storm • Bushfire 	<ol style="list-style-type: none"> 1) For all Incidents requiring an emergency service; (fire, ambulance or police) contact 000 immediately. 2) The staff member who is notified or is aware of the incident must: <ol style="list-style-type: none"> a) Ensure the emergency services are contacted as appropriate. 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; c) The Chief Executive Officer and/or the ECICT must assess whether the incident is an emergency or a non- emergency critical incident. d) building evacuation procedures enacted controlled by the Chief Fire Warden, if appropriate; e) submit an incident report to incident@russo.qld.edu.au; and f) if appropriate, record the incident on client’s file. 3) 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 4) The Chief Executive Officer will convene an ECICT meeting as soon as practicable. 5) If required, Emergency Business Continuity Plan will be enacted by the ECICT. 6) Other offices will be notified by the Chief Executive Officer as required. 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. 8) Dependent on the nature of the incident, a central organizational or external emergency, military services control may occur. 	<ul style="list-style-type: none"> • Formal team debrief • One on one with Manager • One on one with those involved as appropriate • Consider Employee Assistance Program • Review policy and procedure as appropriate
Non-emergency	<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>	<ol style="list-style-type: none"> 1) The staff member who is notified or is aware of the incident must: <ol style="list-style-type: none"> a. Confirm that the incident is a non-emergency and that the emergency services are not required. b. Immediately notify the respective office manager/supervisor; c. Submit an incident report to incident@russo.qld.edu.au; and d. If appropriate, record the incident on client’s file. 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. f. The Chief Executive Officer will notify the police, other offices and third parties as required. 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. 	<ul style="list-style-type: none"> • Formal team debrief • One on one with Manager • One on one with those involved as appropriate • Consider Employee Assistance Program • Review policy and procedure as appropriate

Russo Business School Critical Incident Policy - Response Flowchart



Critical Incident Management Policy

Front of Card
Sarina Russo Group
CRITICAL INCIDENT CONTACT CARD

Life Threatening? → **0 0 0**

Your manager
(if not contatable)
↓
Kathleen 0422 444 722
Newcombe
(if not contatable)
↓
Kevin Anderson 0409 348 544
(if not contatable)
↓
Quentin Underhill 0429 800 814
(if not contatable)
↓
Justin Sharp 0419 709 185
(if not contatable)
↓
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

Back of card
Sarina Russo Group
CRITICAL INCIDENT CONTACT CARD

EMERGENCY 0 0 0

Police Link 131 444
SRI 24/7 1800 994 989

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

Critical Incident Management Policy