Critical Incident Management Policy and Procedure

Policy Owner	CEO
Approving Authority	Governing Council
Implementation Responsibility	CEO
Effective Date	27/08/2021
Review Date	TBA
Current Status	Version 1.0

1. Purpose

The Critical Incident Management Policy and Procedure has three objectives: to address the risks and ramifications that arise from Critical Incidents, to provide relevant and effective responses to Critical Incidents and to implement preventative measures to minimise the risks of Critical Incidents.

This Policy is developed pursuant to the Higher Education Standards Framework (2021), ensuring that Sydney Polytechnic Institute (SPI) meets the requirements under Standard 2, Standard 6 and Standard 7 in the event of a Critical Incident.

- Standard 2 requires SPI to demonstrate that it has readily accessible procedures that cover the immediate actions to be taken in the event of a critical incident and any follow-up required.
- Standard 6 requires SPI to demonstrate that it is operating effectively and sustainably, such as monitoring and taking actions to address underlying causes of Critical Incidents.
- Standard 7 requires SPI to securely and confidentially maintain information that document and record responses to Critical Incidents.

2. Scope

This Policy applies to all SPI staff, students, visitors, contractors and any individual involved in a Critical Incident.

3. Definition

In this Policy, a ***Critical Incident*** is defined as a traumatic event, or the threat of such (within or outside Australia), which causes extreme stress, fear or injury to any individual. Some examples of a Critical Incident include physical harm, psychological harm, property damage, legal incidents, media activity, communicable diseases, natural disasters, civil disorder, overseas incidents or any other unusual activities.

4. Protocols

4.1 Critical Incident Coordinator

4.1.1. The Critical Incident Coordinator (CIC) is authorised by SPI to directly manage Critical Incidents on the SPI premises. The Registrar shall be the CIC unless otherwise delegated by the CEO.

4.1.2. Some of the responsibilities of CIC include:

4.1.2.1. managing the Critical Incident Management Team (CIMT);

4.1.2.2. monitoring the availability of appropriate resources for managing Critical Incidents

4.1.2.3. developing appropriate safety and preventative measures

4.1.2.4. training key personnel to understand and manage Critical Incidents; and

4.1.2.5. maintaining a written record of any Critical Incident and remedial action taken by the CIC in accordance with *the Records and Information Management Policy*.

4.2 Procedure

4.2.1 Phase 1: Prevention

4.2.1.1 To prevent Critical Incidents from occurring, the SPI will conduct a variety of assessments to identify relevant risks and effective preventative measures. The following are some of the actions that SPI will undertake:

a) record risks, mitigation strategies and resultant risks;
b) devise specific plans to reduce the risks identified;
c) conduct annual audits of the resources for managing key risks and report any shortfalls to the CEO;
d) keep the Risks and Prevention Checklist up to date;
e) keep the Immediate Response Checklist up to date;
f) ensure all SPI students, complete the Student Contact Information Form; and
g) ensure a copy of the Student Contact Information Form is placed on the SPI website.

4.2.2 Phase 2: Response

4.2.2.1 If a Critical Incident occurs, any staff member/s directly involved are encouraged to:

a) Promptly assess and protect the physical safety of staff and students. Actions include initiating lockdown procedures or evacuation of the premises;
b) Contact emergency services by calling 000;
c) Contact the CIC at the Institute; and;
d) Consult the Immediate Response Checklist and act accordingly.

4.2.3 Phase 3: Recovery

4.2.3.1 In the event of a Critical Incident, it is the responsibility of the CIC to :

a) Provide those directly affected or responding to the incident with the most relevant and factual information available;
b) Contact the CEO;
c) Debrief or coordinate a debriefing of those directly affected within 8 hours of the Critical Incident occurring, or as soon as possible thereafter;
d) Assess the need for and coordinate counselling or mental support services;
e) Establish or maintain continuous contact with those directly affected by the Critical Incident; and;
f) Assess whether ongoing or additional support from external providers is necessary to address the impacts of the Critical Incident.

4.2.4 Phase 4: Review

4.2.4.1 It is the responsibility of the CEO to review the Recovery and Response measures on an annual basis. In the event of a Critical Incident, reviews are conducted (i) one week, (ii) two months, and (iii) six months following the incident.

(i) The CIC and the CEO will meet within one week of the incident

Purpose of the meeting:

- Provide an update on the Critical Incident.
- Present the findings of the Critical Incident Report, which the CIC will prepare prior to the meeting.
- Discuss the findings of the Critical Incident Report and propose and implement appropriate actions to address the Critical Incident and to improve relevant preventative, recovery and response measures.
- Obtain any relevant legal advice as needed.
- Prepare a report for Risk Committee.

(ii) A meeting with the CIC and CEO must occur two months following the incident.

This meeting will address the following:

- Review the Response and Recovery phase, including any measures taken prior to, during and after the Critical Incident.
- Review the progress of any ongoing counselling or support services, arrange the provision of memorials, manage and reassess resources impacted by the Critical Incident, assist with coronal inquests, assist with any ongoing investigations, etc.
- Review and reassess the legal position of SPI with consideration to the impacts of the incident
- Prepare a report for the Risk Committee regarding the meeting, including any comments, conclusions or recommendations.

(iii) A meeting with the CIC and CEO must occur six months following the incident.

This meeting will address the following:

- Review and suggest modifications of SPI's Critical Incident procedure.
- Prepare a report for the Risk Committee regarding the meeting, including any comments, conclusions or recommendations.

4.3 Risks and Prevention Checklist

4.3.1 Fire

4.3.1.1 Risk

a) The origin of the fire could be internal or external.
b) Some internal fire hazards include faulty electrical equipment, faulty electrical connections, dangerous chemicals, etc.
c) Some locations may have a higher risk of fire, such as student computer rooms, due to the number of electrical devices and connections.

4.3.1.2 Preventive Measures

a) SPI campuses and facilities will maintain and be provided with fire protection measures, including fire alarms, smoke detectors, sprinklers, fire extinguishers, fire escapes and readily accessible building/floor plans in the event of an evacuation.
b) Compulsory fire drills and practice evacuations will be conducted on a regular basis

for all SPI staff and students.

c) Regular inspections of fire measures, such as fire extinguishers and smoke detectors, will be conducted.
d) Emergency contact details, including electricians and emergency services, will be made available to the CIC.
e) Designate Fire Warderns, CIC, First Aid Officers and delegate emergency services personnel.
f) Make known to all staff and students the fire and emergency procedures.

4.3.2 Water

4.3.2.1 Risk

a) Internal origins, such as leaking or damaged plumbing within the building or facilities.
b) External origins, including water damage due to floods, storms or other natural disasters.

4.3.2.2 Preventive Measure

a) Regularly inspect the premises, particularly the computer room or other rooms with a large number of electrical devices.
b) Ensure the building manager's contact details are accurate so the building manager may be easily reached in the event of water leakage.

4.3.3 Criminal Behaviour

4.3.3.1 Risk

a) Behaviour that reasonably threatens the safety of an individual or group. This includes real and threatened physical violence, use of explosives, theft, vandalism, or possession or use of firearms.

4.3.3.2 Preventive Measures

a) Establish and maintain surveillance systems and alarms for use during and outside of operating hours.
b) Ensure that all premises, facilities, and areas under the management of SPI are secured and locked outside of operating hours.
c) Secure all confidential information, physical or digital, and restrict access.
d) Ensure that staff are trained and update their training on a regular basis, or as necessary.
e) Make available emergency contact details for staff and security. Additionally, ensure that the contact details of emergency services are publicly available next to all staff phones and around student areas.

4.3.4 Data / Information Security

4.3.4.1 Risk

a) Failure of ICT systems.
b) Physical damage or destruction of hardware, servers and/or information storage areas.
c) Theft, corruption or destruction of data.
d) Overload or failure of electrical systems.

4.3.4.2 Preventive Measures

a) Regularly backup the System.
b) Maintain a digital copy of all important hardcopy documents.
c) Have offsite document storage.
d) Maintain robust system security, including firewalls and password protection.
e) Lock storage areas and filing cabinets.
f) Invest in secure and high-quality databases.

4.3.5 Pandemics

4.3.5.1 Risks

a) Infection or the exposure of staff and students to the disease.
b) Closure of or restriction of access to facilities.

4.3.5.2 Preventive Measures

a) Provide for effective coordination and communication between all staff and students in the transition to online delivery modes and introduced safety measures.
b) Ensure that all relevant bodies are promptly updated regarding the most recent available health advice or information from the Commonwealth and NSW Health Department. This includes social distancing measures and the provision or mandate of face masks.
c) Coordinate, maintain and, if appropriate, provide financial support for those affected by pandemics or similar situations.
d) Coordinate, maintain and provide mental health support services or counselling for those affected by pandemics or similar situations.
e) Maintain and document the most accurate contact details of all staff, students and visitors.
f) Ensure that a hygienic environment is maintained, and arrange for regular cleaning, disinfecting and ventilation of facilities.
g) Encourage the maintenance of good personal hygiene for all staff and students on campus.

4.4 Communication

During a Critical Incident, effective communication is vital to a successful response.

- It is the responsibility of the CIC to ensure that communication and contact are established and maintained with all relevant parties.
- Information regarding how to seek assistance and incident reporting procedures will be made available to all staff and students.

4.5 Training

- The Critical Incident Management Policy and Procedure, as well as appropriate WH&S training, will be provided to all staff during their orientation and made available upon request afterwards.
- Regular and compulsory emergency evacuation training will be provided to all staff and students. Additionally, any relevant safety information regarding SPI's location and environment will be provided.
- Training for emergency evacuations will be conducted on an annual basis.
- The outcomes of emergency evacuation training will be recorded and assessed.

4.6 Equipment and materials

- Emergency equipment will be checked, maintained and, if appropriate, serviced or replaced on a regular basis.
- At all times, SPI will be equipped with sufficient equipment and material, such as First Aid toolkits, to effectively respond to emergencies and Critical Incidents.

4.7 Useful Documents

- The SPI Organisational Chart (including staff names and positions).
- The Critical Incident Register and/or Report.
- Staff Contact Details and the details of the incumbent Critical Incident Coordinator.
- Student Contact details and lists.
- Emergency Services and Security contact details.
- Suppliers' and affiliates' contact details.
- Evacuation procedures.
- Up-to-date floor plans featuring emergency exits.
- Details of staff with First Aid training.
- Information and details of SPI's Insurance.
- Specifications of IT systems.
- Maintenance agreements.

Notes

Related Documents:

SPI Risk management Policy
SPI Health and Safety Policy
SPI Business Continuity Management Policy
SPI Bullying, Harassment and Discrimination Policy
SPI Workforce Plan

Amendment History:

Version No.	Approved by	Effective date	Amendments
1.0	Governing Council	27/08/2021	New Policy