

## Critical Incident Management Policy

---

### 1. Background

Critical incidents pose a risk to the integrity and business continuity of Gateway Business College's (GBC) higher education operation and higher education course delivery. Critical incidents also pose a risk to the wellbeing and safety of GBC's staff and students, external members of Boards and Committees and visitors to the GBC campus. Critical incident management is part of GBC's risk management framework that identifies potential critical incidents and provides guidelines for the implementation of appropriate measures to address critical incidents that may occur.

### 2. Purpose

This policy outlines an organisational framework for managing critical incidents, including identification, preparation, evaluation, reporting, response and recovery processes. The critical incident management framework establishes measures to ensure GBC maintains a duty of care for the GBC community, including staff, students, members of GBC Boards and Committees, partners, contractors and visitors. In addition, it works to minimise risk to business continuity, higher education operations and course delivery.

### 3. Scope

This policy applies to GBC staff, students, external members of GBC Boards and Committees, partners, contractors and visitors to the GBC campus.

### 4. Definitions

**Business Continuity Plan:** Planning document that identifies threats and risks, and provides a strategy to mitigate the consequences of these risks in order to protect GBC's personnel and assets in the event that an identified threat occurs.

**Corporate Governance Board:** The formally constituted governing body accountable for the governance of GBC as a higher education operation.

**Critical incident:** A major event, episode or crisis that poses a high level of risk to the health, safety, wellbeing or reputation of any person(s) or group at GBC, GBC's higher education operation, higher education course delivery or reputation.

**Duty of care:** GBC's moral and legal obligation to act responsibly to protect the safety and wellbeing of staff, students, members of GBC Boards and Committees, partners, contractors, visitors and other stakeholders.

**Non-academic staff:** Staff employed at GBC in administrative, IT, marketing or student support services roles.

**Risk:** In accordance with the International Standard for Risk Management, risk is the effect of an uncertain environment on the achievement of an organisation's objectives.

# Critical Incident Management Policy

---

**Risk Management Framework:** A suite of documents that outline the processes and procedures for risk management at GBC, including but not limited to the *Business Continuity Plan*, *Compliance Framework Policy*, *Critical Incident Management Policy*, *Risk Management Policy*, *Workplace Health and Safety Policy*.

**Senior Management:** Senior management staff responsible for the day-to-day management of higher education operations at GBC, as delegated by the Corporate Governance Board.

## 5. Principles

GBC must be prepared to respond in the case of an emergency, crisis or critical incident. GBC has a duty of care towards its staff, students, contractors and visitors and as such, ensuring their safety and security is of utmost importance to GBC.

GBC will continually monitor all risks in line with its *Risk Management Policy* and *Business Continuity Plan*. Thus GBC will reduce the risk of a critical incident occurring if possible, and build its capacity to respond quickly and appropriately to critical incidents if they do occur.

### 5.1 Identifying critical incidents

Critical incidents are high risk incidents, different to minor or routine incidents.

Critical incidents include:

- Natural disasters (flood, fire, storm, earthquake)
- Extreme weather conditions or events that may require the closure of the GBC campus
- A fire on the GBC campus
- Telecommunications failure
- Network server failure of more than two (2) hours
- A hostage or siege situation
- The discharge of a firearm
- A serious health threat such as a pandemic, virus outbreak, or chemical leak (liquid or gas)
- A serious accident or injury
- A sexual assault
- Serious physical assault or self-harm
- Serious theft or robbery
- Kidnapping or attempted kidnapping
- The appearance of a bomb or explosive on campus, or a bomb threat
- Any incident that involves a fatality or is potentially life-threatening
- Serious internal fraud
- Industrial action, strikes, riots
- Non-critical incidents with the potential to escalate quickly into critical incidents.

Non-critical incidents, being minor or routine incidents that are not high-risk, include:

- Non-extreme weather
- A small, localised fire that can be contained and extinguished by GBC fire extinguishers

## Critical Incident Management Policy

---

- Minor flooding
- Telecommunications or network outages of less than two (2) hours
- Routine, seasonal outbreaks of colds and flu
- Personal problems
- Bullying
- Harassment
- Minor theft of property
- A minor incident of fraud.

### 5.2 Responsibilities and delegations

The Corporate Governance Board is accountable for the regular monitoring of critical incident management at GBC.

The Corporate Governance Board delegates responsibility for monitoring and reporting on critical incidents to the Audit and Risk Management Committee.

The implementation of critical incident management procedures on campus is delegated to Senior Management and senior staff members.

### 5.3 Audit and Risk Management Committee

The GBC Audit and Risk Management Committee will report to the Corporate Governance Board on all aspects of risk to GBC's higher education operation. A key focus area of the committee will be monitoring, anticipating and responding to risks that have, or could, become critical incidents.

Please refer to the Audit and Risk Management Committee Terms of Reference in the GBC Governance Charter.

### 5.4 Communication

Critical incident management procedures must be clearly communicated to all GBC stakeholders and accessible on the GBC website.

GBC staff and students must be aware of their obligation to act responsibly to protect the wellbeing and safety of themselves and others, and to comply with critical incident guidelines and directives should a critical incident occur.

Should a critical incident occur, stakeholders, including the Academic Board, should be informed immediately and the lines of communication should remain open at all times to ensure those involved or affected are kept informed.

## 6. Procedures

Instructions for emergency response procedures must be clearly displayed throughout GBC campus as part of the security and safety arrangements framework.

Displayed information must include contact telephone numbers for emergency services (Police, Fire, Ambulance) and Gateway Business senior staff members responsible for

# Critical Incident Management Policy

---

critical incident management response; procedure instructions, evacuation directions, basic first aid.

## 6.1 Critical Incident Response

GBC security procedures apply to all critical incidents. Should a serious critical incident that threatens the safety of staff and students occur on the GBC campus, those in the critical incident area must evacuate that area immediately, if it is safe to do so.

At the same time, a senior staff member of GBC must be notified of the critical incident and make an immediate response assessment and act accordingly.

If the incident is potentially dangerous or life threatening or someone is injured, emergency services (Police, Fire or Ambulance) must be contacted immediately on triple Zero (000).

A critical incident may warrant the formation of a critical incident response team. The senior staff member initially notified of the critical incident will make this decision based on the immediate assessment of the incident and in consultation with the CEO.

This team of senior staff members is responsible for the immediate and ongoing management and monitoring of the incident until normal operations resume.

Should emergency services attend the incident, all GBC staff and students are required to comply with their instructions and directions.

Should staff and students be instructed by emergency services to evacuate the building, they must do so immediately. A GBC senior staff member must accompany students during the evacuation process and remain outside with students until the incident is resolved.

Following immediate responses to a serious critical incident, a secondary round of responses must be made by the team of senior staff members. This includes:

- Liaising with emergency services personnel
- Ensuring any physical injuries have been treated by emergency services personnel
- Ensuring any psychological injuries have been treated by emergency services personnel or the student counsellor
- Contacting family members or emergency contacts if required
- Determining the safe and secure resumption of normal operations if possible.

A Critical Incident Response Checklist has been developed to guide appropriate response strategies and activities. See Appendix A of this policy.

## 6.2 Ongoing Response Maintenance in response to serious critical incidents

GBC will continue to monitor the impact of critical incidents that threaten the safety of staff and students. Ongoing response activities include the following support measures:

- Factual information regarding the incident must be made available to all staff and students affected and/or involved
- An official response from the CEO to be communicated to all staff and students
- Counselling services will be provided to those who need it
- Additional support from external agencies will be sought if required

## Critical Incident Management Policy

---

- Debriefing sessions for senior management staff will be arranged
- All physical spaces will be assessed for safety prior to the resumption of normal operations
- The resumption of course delivery will be prioritised.

Documentation will be maintained to ensure a full account of the critical incident, including details of all response strategies and activities, is recorded.

Critical incidents which involve fraudulent behaviour will be responded to in accordance with the *Anti-Fraud and Corruption Policy*.

Procedural plans for dealing with critical incidents that disrupt GBC higher education operations are outlined in the *Business Continuity Plan*.

The GBC CEO is responsible for communication with the media and other external stakeholders in relation to critical incident management. The CEO may consult with the Audit and Risk Management Committee and Corporate Governance Board during this process. Information that is communicated to the media should be accurate and protect the safety and confidentiality of anyone involved, police process or legal process.

Following a critical incident, recovery processes are to be implemented by the Audit and Risk Management Committee, or their delegate/s as per the *Business Continuity Plan*.

### 6.3 Reporting and Evaluation

A record of all critical incidents must be maintained by GBC.

Following a critical incident, a report must be completed by the senior member of staff who was responsible for managing the response to the incident. To ensure accuracy, this may include interviewing staff and students involved.

The Critical Incident Report must include the following:

- Type of critical incident
- A summary of events including the response
- A copy of the completed Critical Incident Response Checklist
- A list of all persons involved in the incident and their role
- Incident outcome and ongoing activity in response to the incident
- Recommendations for improving critical incident response procedures.

The Audit and Risk Management Committee will review all critical incident reports and provide the Corporate Governance Board with a full report and analysis of the critical incident. This may include further investigation including interviewing staff and students.

The Audit and Risk Management Committee Report to the Corporate Governance Board must include the following:

- An analysis of the critical incident, the response and its effectiveness
- Improvement strategies for response procedures
- Identification of any ongoing impact on GBC operations
- Identification of any ongoing risks to GBC
- Risk mitigation strategies
- Recommendations for ongoing response activities if required.

## Critical Incident Management Policy

---

The Audit and Risk Management Committee Report is to be submitted to the Corporate Governance Board for review. Following a critical incident, the Corporate Governance Board will determine the need for a review of the current *Business Continuity Plan* and/or *Risk Management Policy*, and take necessary action as required to achieve this.

GBC must keep a written record of a critical incident for at least two years after affected student/s have ceased to be an accepted student.

### 7. Review

The Corporate Governance Board will review this policy annually, and/or following the receipt of a Critical Incident Report, or at any other time as it deems necessary.

Document History			
Document Name	Critical Incident Management Policy		
Document Owner	GBC	Date Developed	19.11.2016
Initial Approver	GBC Policy Development Committee	Date Initial Approval	23.02.2017
Reviewed by	Governing Board	Date of Approval	17.04.2017
Reviewed by	Governing Board	Date of Approval	12.07.2017
Reviewed by	Governing Board	Date of Approval	05.04.2018
Related documents	Business Continuity Plan Compliance Framework Policy GBC Governance Charter Risk Management Policy Workplace Health and Safety Policy		
Version No.	Summary of Changes		
4.	5.4 Communication: added information (Appended record keeping information on external feedback in reporting and evolution)		

## Critical Incident Management Policy

---

### 8. Appendix A: Critical Incident Response Checklist

Critical Incident Type: Date Critical Incident Manager: Name: Position:		
Incident response: Have you...	Tick	Notes
Assessed the severity of incident?		
Evacuated site (if necessary)?		
Accounted for all staff, students, and visitors?		
Identified injuries?		
Identified damage to property?		
Called Emergency Services? Triple Zero (000): Police, Fire or Ambulance		
Briefed CEO & other senior staff on the situation and what is needed?		
Allocated specific roles and responsibilities to staff?		
Gathered adequate information about the situation?		
Communicated relevant information to staff and students? (ongoing task)		
Recorded decisions and actions?		
Identified key business operations that have been disrupted?		
Communicated relevant information to key stakeholders and external individuals and associations (if necessary)?		
Determined media response if required?		
Completed a Report		