BUSINESS CONTINUITY PLANNING AND INCIDENT MANAGEMENT POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure provides a framework for preparing, establishing, managing, coordinating and evaluating incidents at CQUniversity. The processes set out in this document will assist CQUniversity to:

- demonstrate effective and consistent planning and testing for moderate (critical) and major (crisis) incident

- demonstrate effective and consistent response to any incident
- set the direction for and facilitates the management of any incident
- minimise risk to personnel, property and reputation, and
- implement incident recovery plans.

2 SCOPE

2.1 This policy and procedure applies to incidents which have, or are likely to have, noticeable and detrimental operational impact on CQUniversity, including to:

- employees
- students
- the University Council and Committees
- controlled entities, and
- contractors or third parties acting on behalf of CQUniversity.

2.2 While the Senior Executive will ensure a coordinated response, the safety of life and protection of property and systems is paramount. Localised incident responses will be prepared for and enacted when required, with the Senior Executive notified as soon as reasonably practical.

2.3 This policy and procedure is the official document by which the University clearly communicates:

- support for the business continuity and incident management process, and
- the expected roles and responsibilities of the various committees/groups in the control of business continuity planning and incident management.

2.4 The Vice-Chancellor and President may amend this policy and procedure as appropriate where this document does not fully address the situation at hand.

3 POLICY STATEMENT

Purpose of business continuity

3.1 Business continuity management ensures processes and resources to ensure the continued achievement of critical business requirements.

3.2 Implementing a Business Continuity Management Framework enables the University to:

- recognise the risks and impacts, key resources, and core processes
- plan for unseen or emerging threats to the University over time
- respond to the incident; protect life, property, systems, and other resources
- recover the resources, systems, and processes
- restore to full operations, and
- review response, test preparedness and recalibrate planning.

Purpose of moderate (critical) and major (crisis) incident management

3.3 The purpose of moderate (critical) and major (crisis) incident management at the University is to:

- identify and report incidents
- identify the appropriate procedures to be followed in response to a moderate (critical) and major (crisis) incident
- help students and employees receive appropriate assistance during and following the incident, and

- satisfy governance requirements and ensure reputation preservation.

3.4 The Crisis Management Control Group (CMCG) will coordinate the planning and operational activity of the University's response to any incident in accordance with the Crisis Management Control Group Terms of Reference.

3.5 The CMCG contact details are in the CQUni Phonebook under Emergency Contacts. To manage for digital blackouts, a hardcopy of contact details will be re-printed on a quarterly basis for the Chancellor and Deputy Chancellor and senior and middle management employees.

4 PROCEDURE

4.1 Incidents can occur across, and affect a range of, university processes and resources. The University incident impact categories are:

- people
- facilities, services, and environment
- finance and insurance, and
- reputation.

4.2 Incident examples (linked to the Risk Management Policy, Enterprise Risk Framework and Risk Appetite Statement) include, but are not limited to:

- natural disasters (flood, earthquake, bushfires, cyclones, major storms)
- building fire
- significant chemical, biological and radiological incident
- civil disorder
- industrial accident
- significant financial issue
- significant systems collapse
- terrorism event (bomb threat, building invasion)
- foreign interference
- serious health issue or outbreak of disease or pandemic
- significant adverse change in government policy
- structural instability
- information technology (IT) and cyber security
- electrical
- serious ethical issues such as business and academic fraud, student complaints or major legal issues
- significant or material breach of regulatory obligations under the Tertiary Education Quality and Standards Agency (TEQSA) and the Australian Skills Quality Authority (ASQA)
- non-compliance with accreditation or legislative obligations
- death
- unlawful behaviour including physical and/or sexual violence including Sexual Exploitation, Abuse or Harassment (SEAH) or crime-related incidents such as modern slavery, child abuse
- missing students, or
- significant mental-ill health issues threatening the safety of self or others.

4.3 Incidences in the context of the University's Fire Evacuation Program (FEP) include the following categories:

- fire/smoke (code red)
- medical emergency (code blue)
- bomb/arson threat (code purple)
- internal emergency/lockdown (code yellow)
- personal threat (code black)
- external emergency (code brown)
- evacuation (code orange).

Incident severity criteria is outlined in Appendix 1 – incident severity.

4.4 Incident response and management is outlined as:

Incident Level	Explanation	Response Team	Reporting Team
Minor local	Localised incident managed within local resources with assistance from specific business areas. Note: Ongoing or multiple localised incidents may have cumulative effect and become a major incident.	Emergency Response Team (ERT) Incident Controller: Associate Vice-President, or delegated to Vice-President (Global Development)	ERT Chair
Moderate (Critical)	Key business processes are disrupted, or resources are lost with a moderate or major consequence. The incident may affect external areas.	ERT Incident Controller: Associate Vice-President, or delegated to Vice-President (Global Development)	CMCG Chair
Major (Crisis)	An incident or series of incidents that have the potential to have extreme consequences on processes, resources and the University's long-term prospects or reputation. This incident may affect external areas.	CMCG Incident Lead/Controller: the Vice-President (Global Development), supported by business areas	CMCG Chair

Business continuity

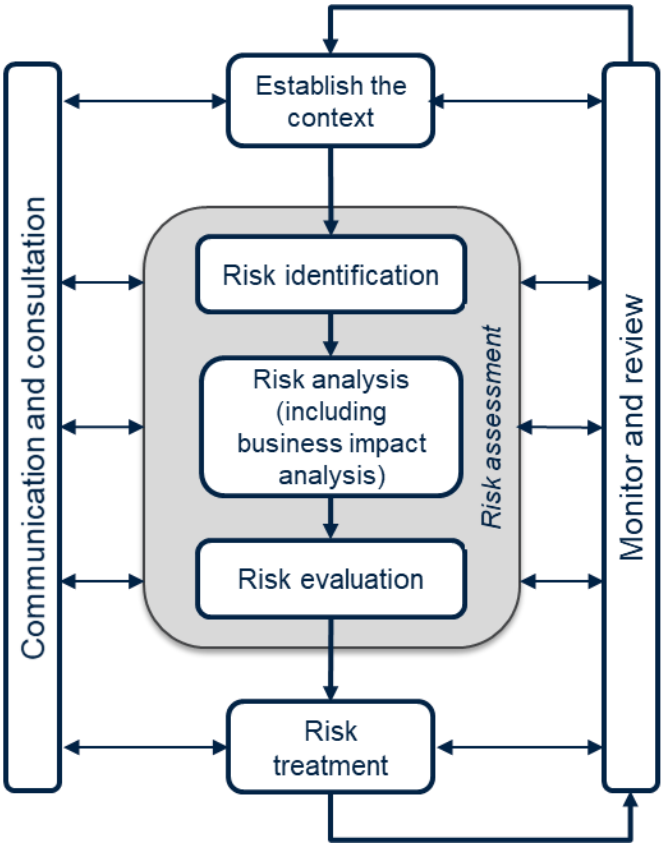
4.5 Business continuity planning addresses the following key questions:

- what could happen?
- what does it mean for the business area, division, University?
- what is critical to continue the University business?
- what must the area, division, University do before, during and after an incident?

4.6 Consideration needs to be given to the management of incidents from a whole of university perspective and requires collaboration between all campuses to plan for and communicate throughout the incident.

4.7 The CMCG is strategically responsible for planning and testing the University's response to potential threat incidents and for reporting any major concerns to the Vice-Chancellor and President for further determination.

4.8 The process for planning incidents that can disrupt the University is:



Business Continuity Process – AS/NZS 5050:2010 Business continuity – managing disruption-related risk

4.9 The Business Continuity Framework sets out the processes and tools required to enable rapid response to incidents, recovery of key processes and restoration to core business activities (Business As Usual) and is based on the preparation of a:

- emergency planning and incident management and recovery
- business continuity plan (BCP)
- disaster recovery planning for critical infrastructure and resources
- communications and media liaison strategies, and
- continuous review and improvement of these documents and processes.

4.10 The BCP defines the approach to dealing with an incident that adversely affects University operations. It details the steps to take to enable rapid response, recovery of key processes and restoration to core business activities. BCPs will detail the following minimum elements:

- scope
- objectives in the context of business continuity
- stakeholders, employees, and resources
- define the external and internal risks against the University risk appetite
- risk analysis
- key processes and consequences
- escalation procedure (maximum acceptable consequence and response requirements)
- instructions for ERT or CMCG
- internal and external communication strategies, and

- scenarios for testing, monitoring, and evaluating the BCP.

Employees must be able to enact the plan with minimal prompting at the time of an incident.

4.11 University-wide BCPs are, and continue to be, developed and maintained for University-wide and campus operations outlined in Appendix 2 - University Priorities Areas for BCPs and on the Business Continuity Planning And Incident Management StaffNet Site.

4.12 Each business area is responsible for developing and managing their own BCP, in consultation with relevant stakeholders. The BCP should include:

- identifying, assessing, prioritising and evaluating risks that could result in significant disruption to the business area, division or University in accordance with the Enterprise Risk Management Framework, Risk Management Policy and Risk Appetite Statement
- developing scenarios and annually test, monitor, and review the BCP readiness
- quality assurance review of the BCP to ensure currency
- demonstrating consultation with relevant stakeholders
- recording information in the relevant University database/s and record management systems
- ensuring employees are up to date with the BCP and steps to take to ensure rapid restoration to business activities, and
- ensuring communication plans developed.

Emergency management

4.13 The Emergency Response Team (ERT) can be activated by the Associate Vice-President (or delegate) or the CMCG Chair (or delegate), except for the Rockhampton North campus, which must be activated either by the Vice-Chancellor and President or Vice-President (Global Development), given the multi campus impact of services delivered through the Rockhampton North campus. Where a Rockhampton North localised incident occurs, the response may be delegated by the Vice-Chancellor and President or Vice-President (Global Development) to the Associate Vice-President to coordinate a response. Where an incident involves non-compliance or a breach with regulatory, accreditation or compliance obligation, the Vice-President (Academic) may also activate the ERT.

4.14 The ERT is responsible for managing incidents at University managed locations in accordance with the Emergency Response Team Terms of Reference.

4.15 ERTs contact details are in the CQUni Phonebook under Emergency Contacts.

4.16 ERT Chair's will report to the CMCG on post incident evaluations/debriefs. The CMCG is responsible for ensuring ERT compliance during incidents.

International incident management

4.17 Risks to safety and health when overseas include personal safety (for example, associated with endemic crime or civil or political unrest) and health related concerns (potential exposure to tropical or exotic diseases).

4.18 When travelling overseas employees and students are to:

- have the International SOS Assistance App downloaded (membership number **12AYCA092257**)
- have a copy of the University or Agent Trip Handbook with the In Country Contact Information clearly marked
- register with Smart Traveller
- have a copy of the travel insurance, and
- have their mobile device on 24/7 and be contactable.

4.19 Notification of incidents:

Minor Local management, with assistance from the University	**Moderate (Critical)** Managed by International SOS, supported by CMCG	**Major (Crisis)** Managed by International SOS, supported by the CMCG
Report to the University within one day	Report to International SOS immediately	Report to International SOS immediately

4.20 If an incident occurs, contact:

- in country support person
- International SOS App or call directly +12159428226, and
- the University.

4.21 When the incident is closed, record the incident via the Report an Incident or Report a Confidential Incident forms in the CAMMS Risk Reporting System.

Moderate (critical) and major (crisis) incident management in Australia

4.22 Where there is an immediate threat to life or property and requires an emergency response:

- call Emergency Services (000)
- activate the Emergency function on the "SafeZone" Mobile App and/or call the Security unit 4936 1331 who will enact the Emergency Notification Alert System (ENAS) in accordance with Appendix 10 – Emergency notification alert system activation guide, and
- enact emergency protocols and/or the building owner/'s emergency procedures as appropriate for leased spaces.

4.23 For moderate (critical) incidents, the Security unit will confirm with the Associate Vice-President the required direction and permission to activate ENAS. In the event of a major (crisis) incident such as active shooter, the Security unit can activate the ENAS directly.

4.24 The CMCG and ERTs are formed as per Appendix 3 – The University's response team roles and responsibilities, Appendix 4 - Incident response team roles and responsibilities, Appendix 5 - major critical incident response with warning flowchart and Appendix 6 - Critical incident response without warning flowchart.

4.25 The CMCG is chaired by the Vice-Chancellor and President on management of the incident until the incident is closed.

4.26 The CMCG will provide the point of interface with other emergency service agencies, such as the Local Disaster Management Group, Police/Fire/Ambulance Services, and Declared Emergency Service Groups on behalf of the University.

4.27 Depending on the incident level, the CMCG and ERTs will identify the severity and consequences of the incident.

4.28 The International Directorate must be involved for all incidents that involve international employees and students onshore and offshore.

4.29 The CMCG and ERT teams will:

- review and complete the Immediate Response Checklist (Appendix 7 – Immediate response checklist)
- review and complete the Ongoing Incident Management Checklist (Appendix 9 – Ongoing management of the incident)
- identify an incident control room (Appendix 8 – Critical incident control room)
- complete an incident record in the CAMMS Risk Reporting System

- maintain communications through regular meetings and briefings throughout an incident, the incident recovery and closure, and
- always maintain records of the incident.

4.30 Communications of moderate (critical) and major (crisis) incidents in Australia will be via the ENAS and other communication channels deemed appropriate by the CMCG.

4.31 Communications of moderate (critical) and major (crisis) incidents overseas will be via the International SOS App and other communication channels deemed appropriate by the CMCG.

4.32 During a pandemic, progression from crisis response, recovery and new normal can happen just as quickly as responding to a natural disaster.

Mass notification

4.33 The ENAS is an emergency messaging system that sends alerts to phones via text messaging, email addresses and other mobile devices, as well as an Emergency Activation System.

4.34 Members of the University community (employees, students, contractors) can notify Emergency 000 and/ or the Security unit if they need assistance or that an incident is occurring, and emergency response is required via the SafeZone App.

4.35 The ENAS will be used only for emergency communication purposes and never for routine communications.

4.36 To minimise the risk of security not being able respond to the alert, and in such an event where the officer is already responding to a request for help, the University has established a backup team to respond. The responder position and timeframe is outlined in Appendix 11 – Emergency notification alert system response guide.

4.37 In addition to the University's ENAS, mass notifications to employees and students travelling overseas will be through the International SOS App and other International SOS communication channels.

Student information management

4.38 Employees may disclose the identity of students to other employees of the University for the purpose of managing and reporting on an incident.

4.39 When the incident is a disclosure of sexual violence, employees may only disclose the identity to the Deputy Vice-President (Students) and University Secretary, and follow the procedures set out in the Student Critical Incident Policy and Procedure.

4.40 The Deputy Vice-President (Students) and University Secretary will manage the disclosure confidentiality and decide whether the student's identity needs to be further disclosed to manage the incident.

Incident closure

4.41 Once the incident is considered closed by the CMCG:

- employees, students, and other people involved will be provided an opportunity to access counselling support, and
- the incident will be reported via the CAMMS Risk Reporting System if it involved a student.

Evaluating incident management and response

4.42 An evaluation must be undertaken when each incident concludes to determine if the activities were successful, for example delivered intended outcomes and met all requirements and identify lessons to be learned.

4.43 The evaluation must be documented and filed in the University's records system for reference when considering future involvement with the same partners or similar agreements.

Training

4.44 The Safety and Wellbeing Unit and Facilities Management Directorate are responsible for, and committed to, delivering incident management awareness training and information to employees and students. Training and information will be accessible via a range of modes, including face-to-face, online and communiques.

Indemnity

4.45 The University indemnifies incident committee personnel against civil liability resulting from workplace emergency response assessment, education, training sessions, periodic exercises, or emergency evacuation of a building where the personnel act in good faith and in the course of their emergency control duties.

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The University Council is responsible for the monitoring and governance associated with key risk activity for the University, which business continuity and critical incident management falls within.

5.2 The Vice-Chancellor and President is accountable to the University Council and has overall responsibility for protecting the University from unacceptable costs or losses associated with its operations and for developing and implementing systems for effectively managing the risks that may affect the achievement of objectives and operational outcomes.

5.3 All employees are responsible for:

- the adoption of risk management and business continuity management practices
- meeting their obligations under relevant legislation such as workplace health and safety, equal employment opportunity, University Code of Conduct, and
- taking all practical steps to minimise the University's exposure to contractual, tortuous and professional liability.

5.4 The effectiveness of risk and business continuity management is unavoidably linked to management competence, commitment and integrity, all of which forms the basis of sound corporate governance. Corporate governance provides a systematic framework within which the executive management group can discharge their duties in managing the University.

5.5 Specific implementation, administration and management including, but not limited to training, maintenance, upkeep and reporting on the FEP and associated emergency plans, and ERTs, is the responsibility of the Safety and Wellbeing Unit and Facilities Management in association with the Associate Vice-Presidents.

5.6 The Safety and Wellbeing Unit will work with the management of controlled entities and the Facilities Management Directorate to ensure that as a minimum, compliant emergency structures and FEP and emergency plans exist and are maintained.

Records management

5.7 Employees must manage records in accordance with the Records Management Policy and Procedure. This includes retaining these records in a recognised University recordkeeping information system.

5.8 University records must be retained for the minimum periods specified in the relevant Retention and Disposal Schedule. Before disposing of any records, approval must be sought from the Records and Privacy Team (email records@cqu.edu.au).

6 DEFINITIONS

6.1 Terms not defined in this document may be in the University glossary.

Table of abbreviations

BCP	Business Continuity Plan
CMCG	Crisis Management Control Group
ENAS	Emergency Notification Alert System
ERT	Emergency Response Team
ESOS	Education Services for Overseas Students
FEP	Fire Evacuation Program
IT	Information Technology
OSHC	Overseas Student Health Cover
SEAH	Sexual Exploitation, Abuse or Harassment

Terms and definitions

Business continuity management framework: sets out the processes and tools necessary to enable rapid response, recovery and restoration to core business activities.

Business Continuity Plan (BCP): comprises many elements which, collectively, define the approach to dealing with a break in business continuity, and which prescribes the steps an organisation should take to recover lost business functions.

Emergency preparedness: arrangements made to ensure that, should an emergency occur, all resources and services needed to cope with the effects can be efficiently mobilised and deployed.

Emergency prevention: measures taken to eliminate the incidence of emergencies. These include the regulatory and physical measures to ensure that emergencies are prevented.

Incident: an event or condition, expected or unexpected, that threatens life or safety and requires immediate action. Please note: multiple or ongoing incidents may have a cumulative effect, becoming a major incident or crisis.

Moderate incident (critical): an event, or series of incidents, that have the potential for extreme impact on employees, students, people, processes, resources and the University's long-term prospects or reputation. For the purposes of international student critical incidents, this is an incident that could affect the overseas student's ability to undertake or complete a course, such as but not limited to, incidents that may cause physical or psychological harm and managed by the Student Critical Incident Policy and Procedure.

Major incident (crisis): an event or outage where key business processes are disrupted, or resources are lost and has a moderate to major impact on the University. This may affect external areas.

7 RELATED LEGISLATION AND DOCUMENTS

Building Fire Safety Regulation 2008 (Qld)

Crisis Management Control Group Terms of Reference

Disaster Management Act 2003 (Qld)

Education Services for Overseas Students (ESOS) Act 2000 (Cwlth)

Emergencies Act 2004 (ACT)

Emergency Management Act 2004 (SA)

Emergency Management Act 2005 (WA)

Emergency Management Act 2013 (Vic)

Emergency Response Team Terms of Reference

Enterprise Risk Management Framework

Fire Evacuation Program

Incident and Hazard Reporting and Investigation Procedure

Information Privacy Act 2009 (Qld)

National Code of Practice for Providers of Education and Training to Overseas Students (National Code) 2018 (Cwlth)

Risk Management Policy

State Emergency Service Act 1989 (NSW)

Student Accommodation including International Students under 18 Policy and Procedure

Student Critical Incident Policy and Procedure

Work Health and Safety Act 2011 (Cwlth)

Work Health and Safety Regulations 2011 (Cwlth)

8 FEEDBACK

8.1 Feedback about this document can be emailed to policy@cqu.edu.au.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Council
Delegated Approval Authority	N/A
Advisory Committee	Audit, Risk and Finance Committee
Required Consultation	N/A
Administrator	Director People and Culture
Next Review Date	29/06/2025

Approval and Amendment History	Details
Original Approval Authority and Date	Council 28/11/2011
Amendment Authority and Date	Council 29/04/2015; Council 27/06/2018; Council 29/10/2020; Audit, Risk and Finance Committee 27/04/2021; Acting Vice-President (Global Development) 07/10/2021; Council 29/06/2022.
Notes	This document was formerly known as the Business Continuity and Crisis Management Policy (last approved 07/09/2016). This document consolidated and replaced the Business Continuity and Crisis Management Policy, Business Continuity Management Procedure, Critical Incident Procedure and Emergency and Fire Evacuation Policy (approved 27/06/2018).

11 APPENDICES

Appendix 1: Incident severity

With the precautionary principal applied, determine the severity of an incident. (i.e., a higher consequence in one category will trigger a higher-level incident).

Consequence/Impact Table					
Risk Categories	**Insignificant** *Some loss but immaterial. Existing controls and procedures should cope with event or circumstance*	**Minor** *Event with consequences that can be readily absorbed but requires management effort to minimise the impact*	**Moderate** *Significant event or circumstance that can be managed under normal conditions*	**Major** *Critical event or circumstance that can be endured with proper management*	**Extreme** *Critical event/circumstance with potentially disastrous impact on business sustainability*
Strategic Risk	• No material effect on objectives	• Temporary or inconvenient delay in objectives	• Marginal under achievement or material impediment to achieving objectives	• Significant under achievement or major delay in achieving objectives	• Non-achievement of objectives
Reputation *Key stakeholders:* • *Students* • *Employees* • *Alumni* • *Government; all levels of domestic and foreign governments* • *Unions* • *Community*	• Ad hoc mentions or rumours of a negative event on social media • Complaint by one or several un-associated members of the general public	• Adverse local and social media coverage for a brief time • Complaint by a group from the community which escalates into the public arena	• Extended negative attention/concern from the public, State media or stakeholders	• Significant continuous attention/concern from the public, national media or stakeholders	• Prolonged and adverse national or international media coverage, undermining public confidence in the University • Government intervention • Irreparable damage to brand • Key stakeholders disassociate themselves from the University
Corporate Risk	• No impact on operations • No impact on student numbers	• Minor and brief impact on non-critical operations • Up to 1% impact on student numbers	• Minor and brief impact on critical operations • Between 1% to 5% impact on student numbers	• Significant impact on critical operations • Between 5% to 10% impact on student numbers	• Significant, irrecoverable impact on critical operations • Greater than 10% impact on student numbers

Risk Categories	Insignificant *Some loss but immaterial. Existing controls and procedures should cope with event or circumstance*	Minor *Event with consequences that can be readily absorbed but requires management effort to minimise the impact*	Moderate *Significant event or circumstance that can be managed under normal conditions*	Major *Critical event or circumstance that can be endured with proper management*	Extreme *Critical event/circumstance with potentially disastrous impact on business sustainability*
Business Disruption and System Failure	• Loss of critical systems leading to business disruption (up to two hours) • Some inconvenience to localised operations • The incidence is absorbed by routine processes and management.	• Loss of critical systems leading to business disruption (more than two hours but less than eight hours) • Inconvenient to localised area but tolerable period • The incidence is contained and absorbed by management intervention	• Loss of critical systems leading to business disruption (more than one day but less than three) • Inconvenient to several business areas for a protracted time but tolerable period. • The incidence may require management intervention to CMCG level but may also be managed, depending on circumstances at Vice president Level as normal business	• Loss of critical systems leading to significant business disruption (more than three days but less than one business week) • Restricted ability to deliver critical services • The incidence requires CMCG Intervention	• Loss of critical systems leading to severe or ongoing business disruption (more than one business week) • Inability to deliver services • Disruption causing campus closure/key business closure for more than one week • Requires immediate Vice-Chancellor and President/Chancellor intervention
Damage to Physical Assets	• Localised damage to a single general asset which can be remediated within a short time timeframe	• Localised damage to a single general asset which can be remediated over a long timeframe. • Widespread damage to a single general asset which can be remediated over a short time timeframe	• Localised damage to a single critical asset which can be remediated over a short timeframe • Widespread damage to several general assets which can be remediated over a short timeframe and /or have financial consequence of up to $500,000	• Localised damage to a single critical asset which may be remediated over a long timeframe • Widespread damage to several general assets which may be remediated over a long timeframe and/or have financial consequence in excess of $500,000 but less than $2 million	• Widespread damage to several critical assets which will must be remediated over a long timeframe • Total and permanent destruction of one or more critical assets with damage in excess of $2 million

Risk Categories	**Insignificant** *Some loss but immaterial. Existing controls and procedures should cope with event or circumstance*	**Minor** *Event with consequences that can be readily absorbed but requires management effort to minimise the impact*	**Moderate** *Significant event or circumstance that can be managed under normal conditions*	**Major** *Critical event or circumstance that can be endured with proper management*	**Extreme** *Critical event/circumstance with potentially disastrous impact on business sustainability*
People and culture	• Increased turnover of personnel or absenteeism of <5%	• Increased turnover of personnel or absenteeism of >5% but <10%	• Localised employee dissatisfaction resulting in an employee satisfaction rating drop of > 10% but <20% • Widespread employee dissatisfaction resulting in employee satisfaction rating drop of <10% • Increased turnover of personnel or absenteeism of >10% but <15%	• Localised employee dissatisfaction resulting in an employee satisfaction rating drop of >20% • Widespread employee dissatisfaction resulting in employee satisfaction rating drop of >10% but <20% • Increased turnover of personnel or absenteeism of >15% but <25%	• Widespread employee dissatisfaction resulting in employee satisfaction rating drop of >10% • Increased turnover of personnel or absenteeism of >25%
Safety and health	• No significant medical treatment required. Any injury which requires first aid treatment but no lost time. • Insignificant impact on physical, psychological or emotional wellbeing	• Any injury which requires first aid treatment –with lost time < 10 days • Minor impact on physical, psychological or emotional wellbeing	• Any injury requiring medical treatment and/or lost time of>10 days and <15 days • Moderate impact on physical, psychological or emotional wellbeing	• Any injury requiring medical treatment and/or lost time of >15 days • Total or permanently disabled • Major impact on physical, psychological or emotional • wellbeing	• Loss of life where the University is potentially at fault or liable
Financial Risk	• Financial loss up to $100K	• Financial loss between $100K to $300K • Internal control weakness that meets 'materiality' threshold for possible disclosure	• Financial loss between $300K to $2m • Adjustment to financial statement disclosure	• Financial loss between $2m to $10m • Multiple significant internal control deficiencies	• Financial loss in excess of $10m • Multiple material weaknesses and financial report restatement
Environmental Risk	• Brief pollution • No impact or measurable impairment	• Transient harm • Minor impact	• Moderate harm • Measurable impact but not affecting ecosystem function	• Significant harm • Serious impact with some impairment of ecosystem function	• Long term harm • Very serious impact with significant impairment of ecosystem function

Risk Categories	**Insignificant** *Some loss but immaterial. Existing controls and procedures should cope with event or circumstance*	**Minor** *Event with consequences that can be readily absorbed but requires management effort to minimise the impact*	**Moderate** *Significant event or circumstance that can be managed under normal conditions*	**Major** *Critical event or circumstance that can be endured with proper management*	**Extreme** *Critical event/circumstance with potentially disastrous impact on business sustainability*
Legal, Compliance and Regulatory Risk	• A one-off breach of a policy or procedure with negligible impact to the University's operating environment identified through immaterial breakdown of control and identified through operating processes	• A minor breach of policies and procedures, occurring more than once which results in a warning but not of a breach of laws and/or a regulator warning • The breach requires some modification to the operating environment	• A breach of any laws, regulations, contracts or licences, including notifiable incidents resulting in active monitoring by a regulator • A significant breach in operating policies or procedures and result in significant breakdown of control environment	• A major continued breach of policy and or process discovered by audit review • A major breach resulting in: o Civil penalties <$1M o Show cause notices from Regulator o Loss of licence o Enforceable undertaking o Significant and system breach of University policy documents	• A total systemic system failure and breach resulting in: o Prosecution with the potential for executives to be imprisoned o Civil penalties >$1m o Loss of critical licence/ accreditation
Major Project Risk	• <1% of project budget • Little or no delay • Either party is irritated but no formal complaints	• 1 to 5% of project budget • Short delay/duration increased >2% • Resolved at working level	• 5 to 10% or project budget • Significant delay / duration increased >10% • Resolved at senior management level	• 10 to 25% of project budget • Major delay / duration increased >25% • Divisional Head intervention	• >25% of project budget • Project halted • Major delay / duration increased >50% • Legal recourse initiated
Local Incident Management	**Minor Incident** Local Management, with assistance from relevant business areas. Reported to Associate Vice-President.		**Critical local Incident** Managed by Associate Vice-President and their ERT. Reported to and assisted by appropriate business area and CMCG		**Major Critical Incident (Crisis)** Reported to and managed by CMCG. ERT to support localised management if required.

Appendix 2: University prioritiy areas for Business Continuity Plans (BCPs)

The following areas have been identified as University priorities for a Business Continuity Plan (particularly as they are linked to each other in many cases). The managers of controlled entities will also need to ensure that a similar approach is taken for these priority areas (where in existence) for their own business areas. For some areas, including group crisis management, and media/communication strategies, participation in a University-wide solution is required.

Please note the descriptions below are simplistic – this is a high-level framework only.

Business Continuity Plan (BCP) 1 – Campus operations

Process Owners: Vice-President (Global Development) and Vice-President (Academic)
Responsible Managers: Director Facilities Management and Director People and Culture

University campuses are the hubs of learning and teaching delivery, research activity, engagement work and the day-to-day operations of the University. There are various 'threats' (natural or man-made), which could cause a full or partial disruption to the operations of or access to any of these campuses. Appropriate business continuity and incident planning needs to be in place to ensure that these disruption events can be managed quickly, with regard to the safety of life and property being the highest priority. Another threat is the capacity to deliver learning and teaching during and after a disruptive event and the University's ability to rapidly pivot to online learning to enable students to continue studying with minimal impact. It is recognised that some sites are entirely contained within a single building, such that the loss of access to or operation of that site would constitute full closure.

Specific 'Emergency Management' protocols are details separately in the associated processes contained within the Fire Evacuation Program; however, they are very much linked.

Business Continuity Plan (BCP) 2 – Core IT systems

Process Owner: Vice-President (Global Development)
Responsible Manager: Deputy Vice-President (Digital Services)

University core Information Technology (IT) systems will focus on supporting the University's core business of engagement, learning and teaching, research and innovation and engaged enterprise. As such, it is imperative that appropriate measures are put in place to quickly rectify any disruption to IT services across all our campuses and learning delivery sites.

Disruption recovery planning is a key requirement in this area, and continuous efforts must be made to ensure that successful enactment of this requirement can be undertaken quickly, to reduce the flow on effects of disruption. Obvious linkage to campus operations, thus plans need to take this into account.

Business Continuity Plan (BCP) 3 – Financial operations

Process Owner: Vice-President (Student and Corporate Services)
Responsible Manager: Vice-President (Student and Corporate Services)

The ability to conduct transactional business (both inwards and outwards) is critical for the operations of any university, let alone the University. Business continuity planning in this regard needs to consider activities including accounts receivable, accounts payable, treasury and banking, financial and management reporting (non-exhaustive). Obvious linkage to core IT systems, thus plans need to take this into account.

Considerations of fraud and other like inappropriate activity must also be considered and will utilize existing structure/implementation for internal audit, tracking and management control.

Business Continuity Plan (BCP) 4 – Payroll and human resource systems

Process Owner: Vice-Chancellor and President
Responsible Manager: Director People and Culture.

Our employees are the key to delivering the University's promise to our stakeholders and for meeting the University's strategic aspirations regarding engagement, learning and teaching, research and innovation and engaged enterprise. As such, the University has an obligation to ensure that employees are not personally affected by a disruption to payroll activities.

Obvious linkage to campus operations, core IT systems and financial operations, thus plans need to take this into account.

Business Continuity Plan (BCP) 5 – Academic Delivery

Process Owner: Vice-President (Academic)
Responsible Manager: Respective Deans and Deputy Vice-President (Vocational Education and Training).

Our students are the fundamental reason for our existence and protection of the learning environment and delivery of education through appropriate environments and systems remains critical to the continued success of the business of the university. They are key to delivering the University's promise to our stakeholders and for meeting the University's strategic aspirations regarding engagement, learning and teaching, research and innovation and engaged enterprise. As such, the University has an obligation to ensure that students are not personally disadvantaged by a disruption to education activities.

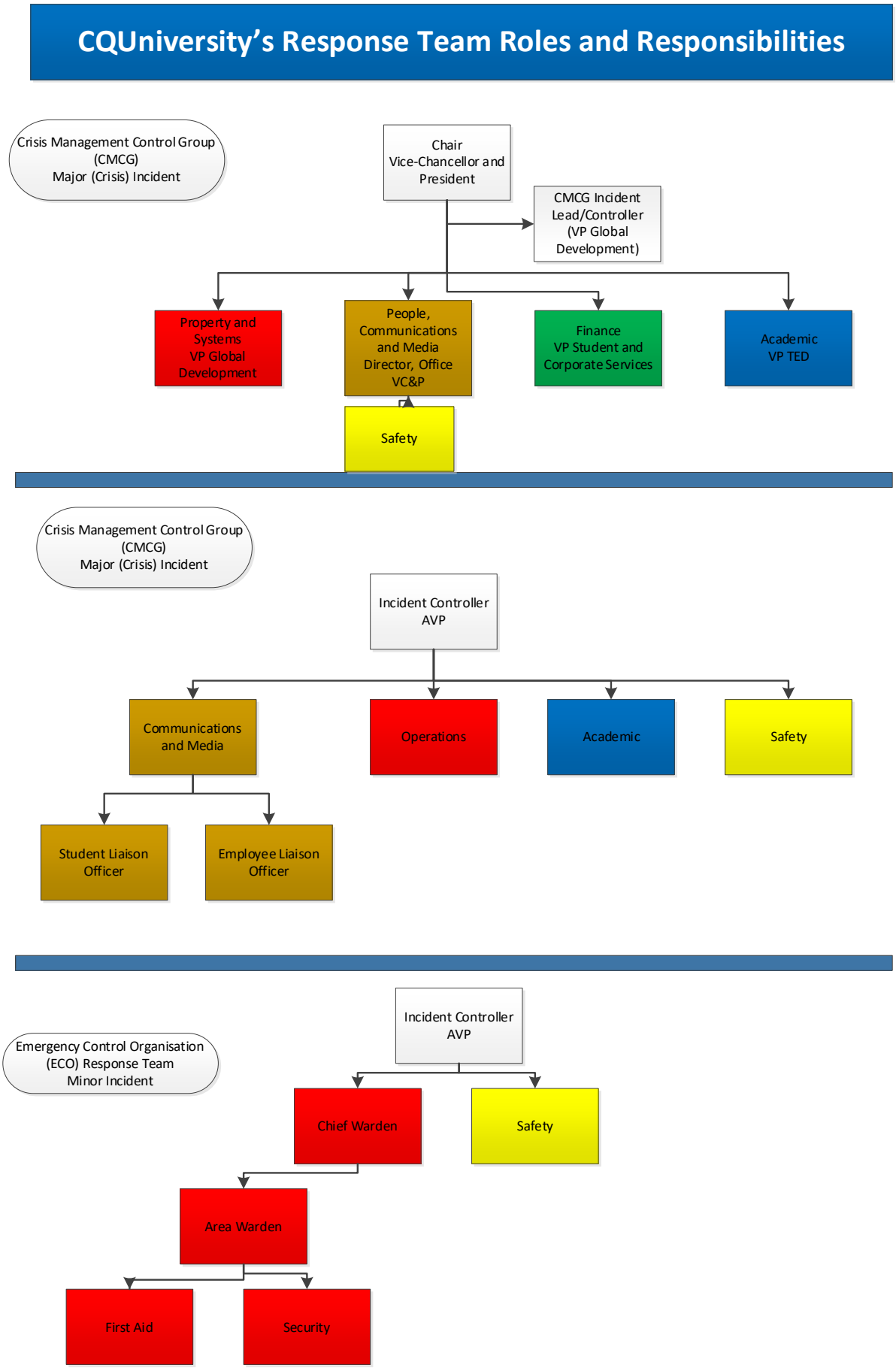
Obvious linkage to campus operations, core IT systems and financial operations, thus plans need to take this into account.

Business continuity plans – other areas

The 'priority list' does not, nor shall it preclude any other areas of the University or controlled entities from understanding the key inputs, processes and outputs of their day-to-day business in order to build a business continuity management culture University-wide. All areas of the University are encouraged to utilise this framework to build resilience for their respective work areas.

All Business Continuity Plans can be found on StaffNet.

Appendix 3: The University's response team roles and responsibilities



Appendix 4: Incident response teams' roles and responsibilities

Role	Incident Type	Who	Responsibility	Placard Colour
Incident Controller (Vice President (Global Development) Supported by: Deputy Incident Controller (Director People and Culture)	Major	Vice-Chancellor and President - Chairs CMCG Vice President (Global Development) - Incident Controller	Incident Controller consults the relevant Response Team and determines the desired outcomes of the incident. Incident Controller takes control and manages the incident by not becoming involved in a 'hands-on" manner, but by managing and leading resources: • assume control • establish a control point • conduct risk assessments • develop incident action plan • determine crisis structure and communication • deploy resources and record details	White
	Moderate	Vice-Chancellor and President - Chairs CMCG Vice-President (Global Development) - Incident Controller		
	Minor	Associate Vice-President		
Communications and Media	All levels	Director Strategic Engagement	Information and warnings Media University community liaison • obtain information on current and projected incident situation. • issue warnings and information to threatened people or University communities. • disseminate incident information to threatened people or University communities. • liaise with media and manage media needs, including social media. Development of a communications plan: • who needs to know what? • how do we let them know?	Brown
Safety Officer	Major	Safety and Wellbeing Manager (or delegated officer)	Reports on all aspects of potential and current safety and risk management issues identified at the incident.	Yellow
	Moderate		Reports on issues related to safety, health and welfare at an incident.	
	Minor			
Finance Officer	All levels	Vice-President (Student and Corporate Services)	Responsible for all financial, administrative and cost analysis aspects of the incident.	Green
Operations	Major	Vice-President (Global Development)	The tasking and application of resources to achieve resolution of an incident. • supervise operations • determines need and request for additional resources • deploys resources • provides first –aid and medical response • establishes and maintains incident command centre	Red
	Moderate	Vice-President (Global Development)		
	Minor	Chief Warden		
Academic	Major	Vice-President (Academic)	• Responsible for any academic issues relating to the incident.	Blue

Business areas that can assist:

Facilities Management Directorate - buildings, estate and vehicles

People and Culture Directorate – employee and student safety

Commercial Services (Bird Cage, 200 Degrees Catering and Student Residences) – meals and accommodation

Tertiary Education Division – Schools and learning and teaching

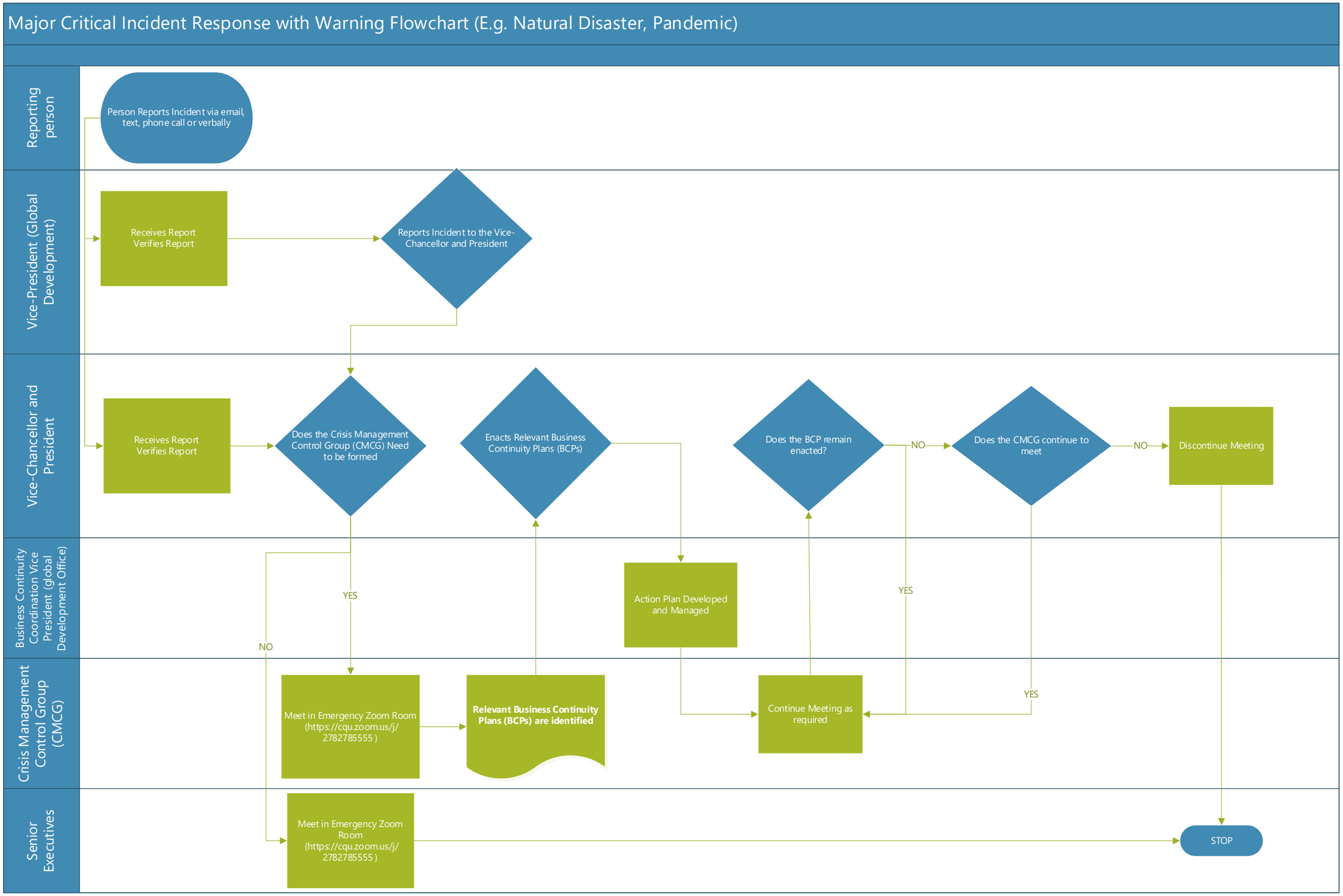
Research Division – Research

Strategic Engagement Directorate – all communications

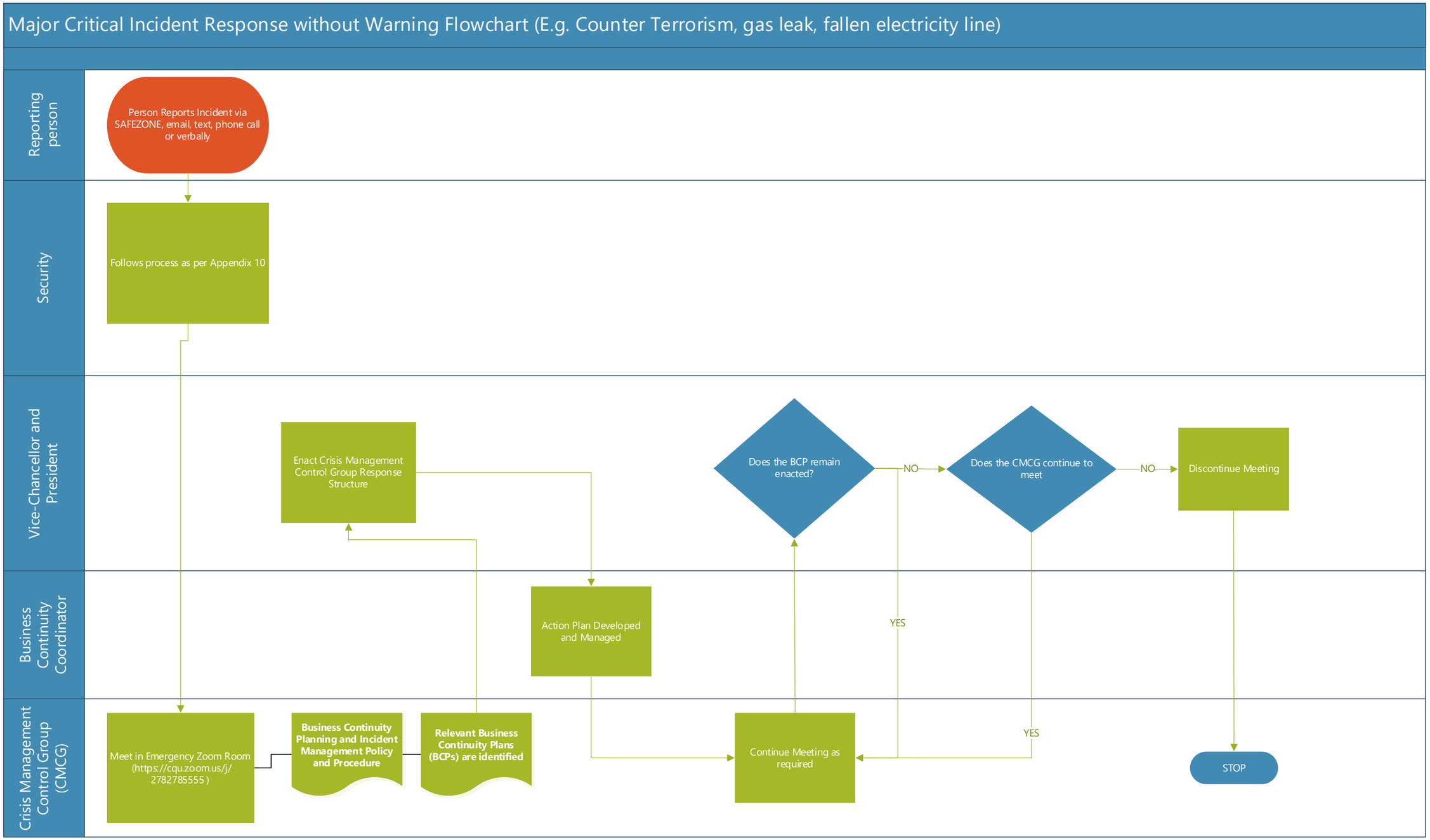
Digital Services Directorate – IT systems

Students and Corporate Services Division – finances and student support and safety

Appendix 5: Major Critical Incident Response with Warning Flowcharts



Appendix 6: Major Critical Incident Response without Warning Flowcharts



Appendix 7: Immediate response check list

Check	Description
	Identify students and employees (and others) closely involved, and therefore most at risk - those directly involved - personal friends/family of those involved - other employees/students
	Determine as a priority - any resources required to manage the incident - if any specialist employees are required to join the Critical Incident Team
	University contacts - Vice-Chancellor and President and Senior Executive - relevant functional managers
	Contact with next of kin/emergency contacts/significant others - what is the most appropriate method of contact?
	Arrangements for informing employees and students - briefing appropriate functional areas - wider audience may not be immediately appropriate, especially if a police matter - guidelines to employees about what information to give to students - written bulletin to employees if the matter is complex
	Managing media/publicity - Is an immediate media comment required, and what will it be?
	Arrange a time and place for an initial group or individual debriefing session with counsellors - employee assistance program - student counselling
	Plan ongoing feedback and regular meetings so that the Critical Incident Team is continually in touch and working together

Questions to consider:

- What is the nature of the incident?
- Is first aid required? Are emergency services required?
- Who is involved?
- What happened?
- When did the incident occur? Is it still in progress?
- Where did the incident occur (or is occurring if still in progress)?
- What actions have already been taken?
- What further actions are required?
- Who needs to be informed? Who has already been informed?
- Who has already engaged in actions to manage this incident?
- Has security been alerted?
- Is media comment required?

Appendix 8: Critical incident control room

Region	Locations Options
Rockhampton	Vice Chancellors Boardroom – Building 1/LG Council Room – Building 10/Level 1 Security Office Boardroom – Building 3/G
Mackay	Campus Administration Building 750/751 CQ TAFE Conference Room Level 4, A Block, CQ TAFE 90-92 Sydney St
Gladstone	LZB Boardroom Adjacent offices building 603
Bundaberg	Campus Boardroom 401/1.12 Vice-Chancellor's Office 404/1.13 Campus Computer Labs 401/1.11, 405/G.03 Meeting Room 408/G.02
Brisbane	Campus Meeting Room Level 8 Chancellery space
Sydney	Campus Boardroom Level 6, Campus
Melbourne	Campus Boardroom Level 1, CBD Campus
Perth	Campus Boardroom Level 4 Room 404 Campus

Appendix 9: Ongoing management of the incident

Check	Description
	Coordinate the access of background information on the student/s such as attendance, academic transcripts, assignment submission, program status etc.
	Ensure the support provided remains timely, relevant and appropriate to the situation, but is also helpful to the student.
	Assess and coordinate the support offered to the friends and family of the student/s affected by the critical incident. May include emergency accommodation, air travel, financial support etc.
	Liaison with police, doctors, hospital employees, insurance matters (e.g. OSHC), immigration, agents
	Consideration of personal items and affairs (household and academic)
	If applicable, arrange access to consultant/representatives from a relevant multicultural or Indigenous
	Keep a record of the formal student sessions/meetings and follow up interviews; for example, attendees,
	Continue to liaise with relevant University employees, students and associated parties as required until the critical incident is brought to an appropriate resolution.
	Death notices, funeral/memorial service arrangements
	Fees issues to be resolved if student cannot continue with their studies (e.g. refund of student's term fees to pay repatriation or associated expenses).
	Arrangements for further counselling/debriefing sessions for groups/individuals as required
	Condolence letters to family
	Running report of all events during the incident – for reporting to Senior Executive

Outside assistance:

- Employee Assistance Program (EAP) – refer People and Culture Directorate
- Student Counselling Providers – refer Students Directorate
- Overseas Student Health Cover (OSHC) Providers – refer International Directorate
- Interpreters, Consular Assistance, Multicultural Groups – refer International Directorate, and
- Indigenous Groups for Support and Assistance – refer Office of Indigenous Engagement.

Principles of action and response:

1. Offering immediate assistance where possible, but avoiding making false promises
2. Being patient, and prepared to explain things, or answer questions more than once
3. Treating all questions seriously and offering truthful answers as soon as possible
4. Identifying what a student's specific needs are and help them develop a plan of action
5. Connecting and referring to support systems within CQUniversity and externally
6. Paving the way for students to return to routine study activities as soon as possible

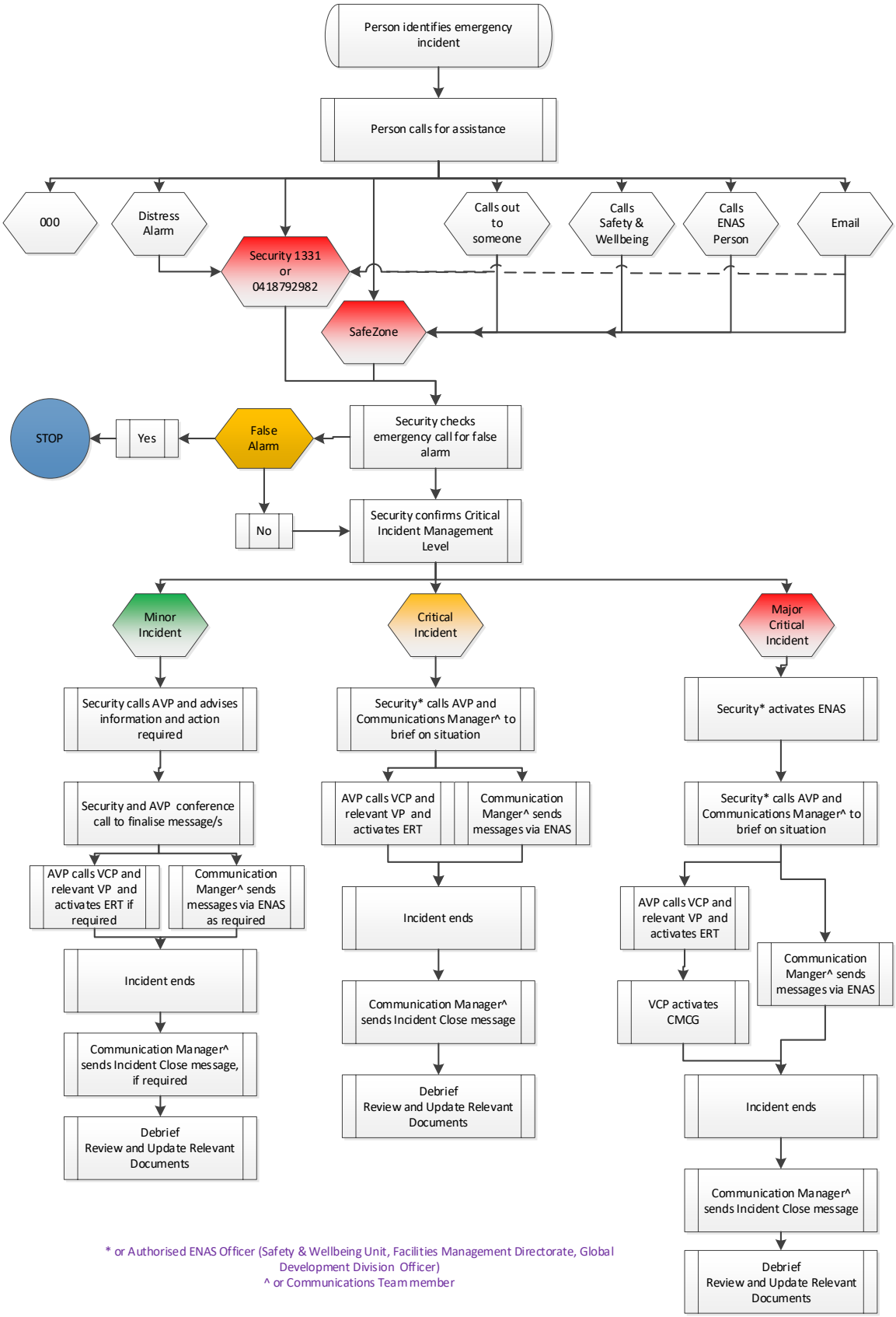
(Adapted from the New York State Office of Mental Health Disaster Resources Website)

Emotions relating to critical incidents:

During or post critical incidents, affected persons may experience:

- a range of emotions, including shock, grief, sadness, anger, apathy or mood swings
- changes in how they think, concentrate and process information
- physical symptoms, such as headaches, fatigue, difficulty breathing etc., or
- a typical behaviour, including outbursts, acts of aggression or social withdrawal.

Appendix 10: Emergency Notification Alert System (ENAS) activation guide



* or Authorised ENAS Officer (Safety & Wellbeing Unit, Facilities Management Directorate, Global Development Division Officer)
^ or Communications Team member

Appendix 11: Emergency Notification Alert System Response Guide