EDITH COWAN UNIVERSITY

Strategic & Governance Services Centre

Critical Incident Management Plan

Version	1.0
Relevance to	ECU Staff
Responsible staff	Chief Risk Officer
Responsible area	Strategic and Governance Services Centre
Date introduced	June 2021
Date(s) modified	September 2025
Next scheduled review date	November 2027
Related University documents	Policy PL202: Critical Incident and Business Continuity Management Enterprise-Wide Business Continuity Plan Critical Incident and Business Continuity Management Guidelines Policy PL201: Integrated Risk Management Work Health and Safety Incident Reporting and Investigation Guidelines Emergency Management Plan Crisis Communications Plan Student Significant Incident Procedure
Related legislation and Standards	AS/NZ ISO 22301:2019: Business continuity management systems

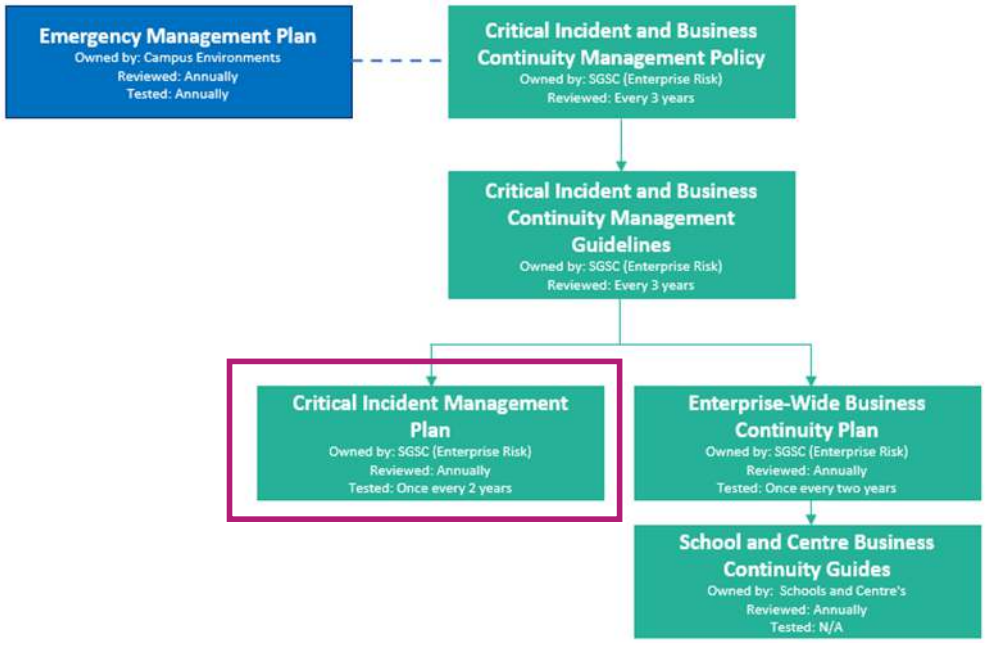
Table of Contents

1. PURPOSE

The purpose of the University's Critical Incident and Business Continuity Management ('CIBCM') framework is to provide a coordinated response to dealing with, and continuing business operations during a Major or Critical incident.

The Critical Incident Management Plan ('CIMP') exists to support the University's Critical Incident Management Team ('CIMT') in providing a consistent approach to responding to a Major Incident or Critical Incident. The **CIBCM Framework Overview** below provides an overview of the University's CIBCM document framework.

Figure 1: CIBCM Framework Overview



2. CRITICAL INCIDENT CLASSIFICATIONS

Incidents at ECU are categorised into one of three levels depending upon the level of support and resources required to manage the outcome. The CIMP will only be activated in a Level 1 Critical Incident, or a Level 2 Major Incident. These category levels and incident criteria are detailed in the **Criticality Matrix**.

Figure 2: Criticality Matrix

Level 1 – Critical

University operations have been critically impacted in one or more areas; or poses a significant risk to the continuity of core University-wide operations

- CIMT convened
- Response led by Recovery Director
- Response in accordance with the Critical Incident Management Plan
- Enterprise-wide Business Continuity Plan activated if required

Level 2 - Major

Major impact on operations of a specific School, Centre or campus location

- CIMT convened at discretion of VP(CS) or a DVC
- Response led by member of University Executive
- Response in accordance with Critical Incident Management Plan
- Enterprise-wide Business Continuity Plan activated if required

Level 3 - Significant

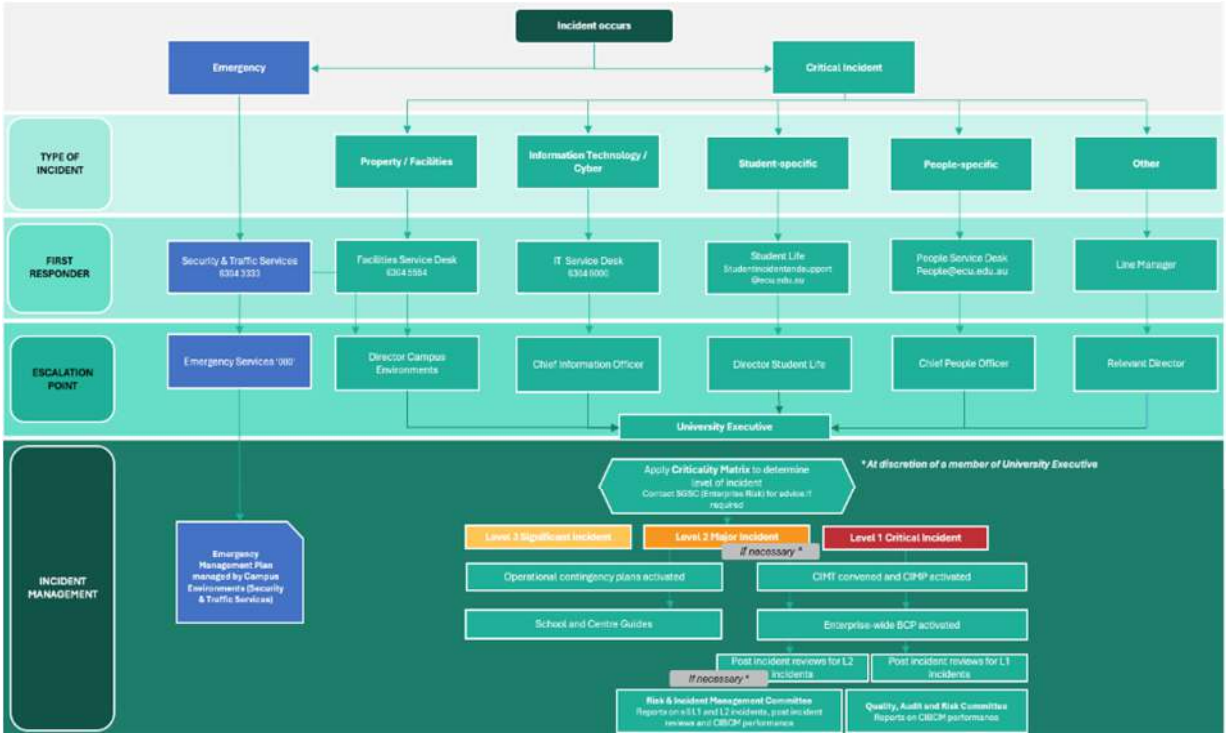
Operational disruption limited in scope or severity and limited impact on wider University

- School or Centre led
- Response led by Executive Dean or Director
- Response in accordance with Operational Contingency Plans
- School or Centre Guides provide business continuity guidance

3. CRITICAL INCIDENT MANAGEMENT PLAN ACTIVATION AND ESCALATION

Incidents occurring at ECU will vary in nature and severity and any impact will depend upon the geographical location, the potential to cause harm to people and the environment, and any economic or reputational impact upon the University. The **Critical Incident Management Process** is illustrated in Figure 3.

Figure 3: Critical Incident management process



Please refer to the Emergency Management Plan, owned and managed by Campus Environments, for the control room procedures in the event of an emergency.

4. CRITICAL INCIDENT MANAGEMENT TEAM

The **Critical Incident Management Team ('CIMT')** is an incident specific team which is formed at the time a Major Incident or Critical Incident occurs and lasts until no longer required. The CIMT does not attend the incident scene but will appoint a Site Liaison to attend the scene if required.

The CIMT will generally comprise of the individuals outlined in Table 1. The nominated alternates will provide assistance and/or step in if needed if a Critical Incident goes over an extended period of time.

Table 1: Critical Incident Management Team

Role	Key responsibilities
Recovery Director *(Vice President (Corporate Services), or the Provost or a relevant Deputy Vice-Chancellor/Executive delegate)*	• Ensure effective management of the CIMT. • Ensure control of all organisational and operational implications. • Maintain communication flows with key stakeholders.
People and Culture Coordinator *(Chief People Officer, or alternate, Chief Safety Officer)*	• Advice on people related issues, including work health and safety. • Maintain appropriate staff counselling, welfare and recovery services and protocols.
Student Support Coordinator *(Director Student Life, or alternate, Manager Student Incident & Support)*	• Advice on student issues including student support needs. • Maintain all appropriate student counselling, welfare and recovery services and protocols.
Physical Resources Coordinator *(Director Campus Environments, or alternate, Senior Manager, Building and Services)*	• Advice on physical resources / asset issues related to a crisis. • Work jointly with People and Culture Coordinator / Student Support Coordinator on any complementary crisis issues.
Information Technology Coordinator *(Chief Information Officer or alternate, Manager Digital Governance, Security, Risk & Operations)*	• Support IT readiness for the crisis and support processes. • Manage IT recovery issues where required.
Communications Coordinator *(Manager Corporate Communications or alternate, Chief Growth Officer)*	• Ensure that the communications strategy and protocols are ready to respond. • Provide advice on appropriate communication strategies to employ. • Coordinate all crisis-related internal and external communications. • Ensure adequate crisis media training for nominated spokespeople.
Governance and Compliance Coordinator *(Director Strategic and Governance Services or alternate, Manager Legal and Integrity)*	• Advice on legal, compliance, risk, regulatory, or academic governance matters. • Advice or reporting to external regulatory bodies.
CIMT Support Coordinator *(Chief Risk Officer or alternate, Senior Risk Adviser)*	• Ensure effective administrative support to CIMT. • Provide advice on enactment and content of Critical Incident Management Plan and/or Business Continuity Plans • Maintain communication flows with key stakeholders. • Organise CIMT meetings, document and record actions and follow-up.

Depending on the type of incident that has occurred, the CIMT may not require all participants, or may require additional participants, including those from external agencies.

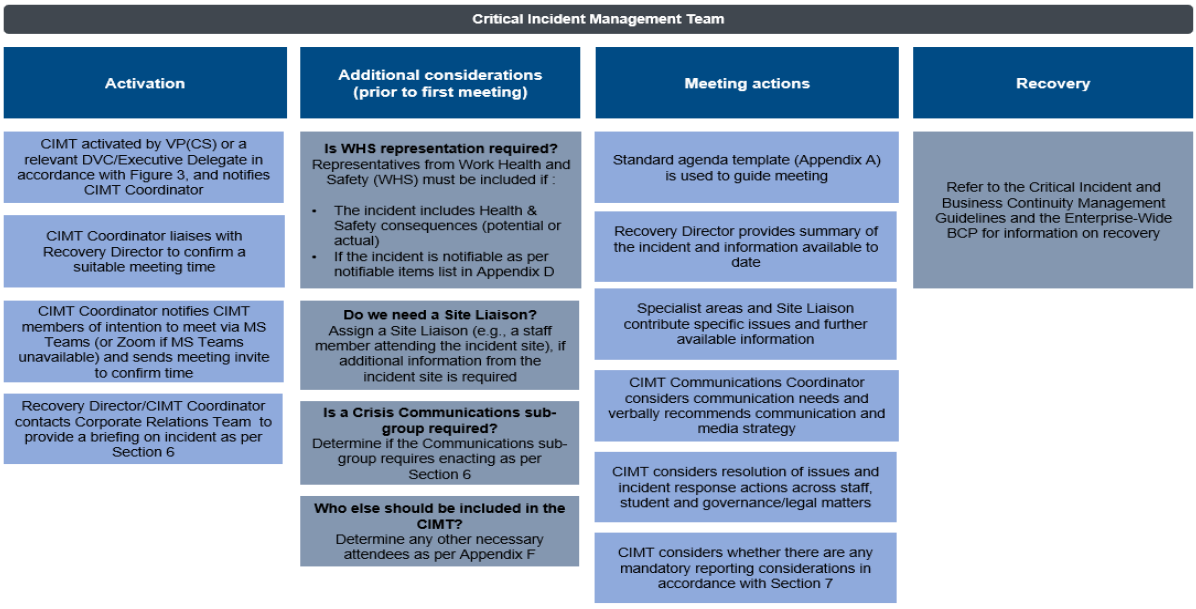
Appendix F provides an overview of the membership of the CIMT which may vary depending on the nature of the incident being managed.

5. COORDINATION OF CRITICAL INCIDENT MANAGEMENT TEAM RESPONSE

In the event of a Critical Incident, the CIMT will meet face to face it possible, or virtually, typically via Microsoft Teams. A Microsoft Teams Channel exists for the Critical Incident Management Team, with all members of the Critical Incident Management Team invited as members. The Teams channel can be accessed here: Critical Incident Management Team (CIMT) | General | Microsoft Teams

In the event of a Critical Incident, the quickest way to get in contact with the CIMT is via this Teams channel, either via the Chat or Meetings functionality. **If Microsoft Teams is not available,** the CIMT is to use Zoom to connect virtually. Instructions on how to set up a meeting using Zoom are outlined in **Appendix B**. The process to activate and coordinate the CIMT is illustrated in Figure 4 below:

Figure 4: Critical Incident Management Team process



6. CRISIS COMMUNICATIONS

Timely, accurate and targeted delivery of communications during a disruption is key to ensuring an incident is managed and controlled appropriately. Crisis communications are planned and managed in accordance with the Crisis Communications Plan which is owned and managed by the Corporate Relations team.

6.1 Initial contact

Once the CIMT is activated, the Recovery Director is to contact the Corporate Relations team to provide an overall briefing on incident. Corporate Relations can be contacted on the after-hours mobile (0492 488 986). If there is no response within an hour, escalate to the Chief Growth Officer (0405 188 456).

6.2 Escalation to subgroup

For Critical Incidents (L1), it may be necessary for a Crisis Communications subgroup of the CIMT to be convened remotely after the initial CIMT meeting, to discuss communication requirements in further detail. The escalation to forming a Crisis Communications subgroup is to be determined in consultation with Recovery Director and the Corporate Relations Team.
A Critical Incident will usually require a Crisis Communications subgroup if the following is required:

- There is a need for key messaging via staff or student via global email;
- Mass communications are required;
- Media needs to be engaged/have contacted ECU; or
- Pro-active messaging is required to protect ECU's brand or reputation.

Please see the Critical Incident and Business Continuity Management Guidelines for further details on what the crisis communications subgroup is responsible for, and who it comprises of.

6.3 Crisis communication protocols

The Crisis Communications subgroup will provide feedback on style and content of official university communications, typically comprising key messages, staff communications and media statements.

Approval of communications

Final approval is provided by the Vice-Chancellor, Vice-President Engagement or relevant Recovery Director.

For speed of response and distribution in a fast-moving crisis, the majority of communications, particularly when operational or ongoing, are attributed to the Vice-President Engagement or the relevant Recovery Director.

Communications will typically direct media related enquiries to the Corporate Relations Manager.

Other ECU teams (Student Life, Digital Services, Campus Environments, Development and Alumni Relations, etc.) are encouraged to distribute approved official university communications on their channels.

The Vice-Chancellor is to be attributed at the beginning or resolution of crisis or for emphatic messaging.

6.4 Crisis communication channels

The approved crisis communication channels are:

- **Mobile phone:** for initial alert and escalation of critical incidents
- **Email:** for approval trails of documents
- **SharePoint:** for document sharing, editing and version control
- **MS Teams:** for sharing of time sensitive but non-critical information during crisis.

Refer **Appendix E** for the approved Communications Matrix.

6.5 Escalation to Council

The Recovery Director and the CIMT will determine if there is a need to notify Council. If an incident is likely to result in significant media coverage, Council must be notified.
Messaging to Council to include:

- Whether they should respond to any media queries they receive, and if determined that they are to respond, what ECU's messaging will be, or alternatively, who media queries should be directed to;
- How frequently the CIMT will update Council; and
- Notification of the incident's close.

During Critical Incidents, the Corporate Relations Team will operate in shifts covering 7.30am-6.30pm 7 days a week as required.

7. MANDATORY REPORTING CONSIDERATIONS

Some Critical Incidents have mandatory reporting obligations which must be considered as part of the overall response. These are outlined below:

A. TEQSA Material Change Notifications

Under the *Tertiary Education Quality and Standards Agency Act 2011*, registered higher education providers must notify TEQSA of an event that will significantly affect the providers ability to meet the Threshold Standards. The notification must be given no later than 14 days after the day the provider would reasonably be expected to have become aware of the event.

The *TEQSA Material Change Notification Policy* requires notification of changes that may impact students, including:

- Critical Incidents and other material breaches in safety; and
- Recurring incidents of sexual assault or sexual harassment.

TEQSA defines critical incidents as a traumatic event, or the threat of such (within or outside of Australia), which causes extreme stress, fear or injury.

The CIMT will determine if the Critical Incident is a notifiable event. If deemed notifiable, the CIMT Recovery Director will work alongside the Director, Strategic and Governance Services to submit the notice via materialchanges@teqsa.gov.au. The CIMT Support Coordinator will retain the records.

Further information on the policy and its requirements can be found here.

B. If an International Student Under 18 is Involved

Under the *National Code of Practice for Providers of Education and Training to Overseas Students 2018*, registered training providers are required to provide certain support in a critical incident.

The National Code is a legislative instrument made under the Education Services for Overseas Students Act 2000 and sets nationally consistent standards to support providers to deliver quality education and training to overseas students.

The National Code defines a critical incident as 'a traumatic event, or the threat of such (within or outside Australia), which causes extreme stress, fear or injury'. The critical incident policy must be activated in these situations. This does not include serious academic misconduct.

In all instances where a Critical Incident involving an under 18-year old International student has occurred the University will, depending on the circumstances, inform and consult with the following individuals and agencies:

- Parent or legal guardian
- Department of Home Affairs
- WA Police
- Department of Communities (WA)
- ECU Counselling services

As per the Code, ECU will maintain a written record of any critical incident and remedial action taken by the University for at least two years after the overseas student ceases to be an accepted student under the ESOS Act.

Further information on the Code and its requirements can be found here.

C. Data Breach

The University must comply with the Australian Privacy Principles, contained within *the Privacy Act 1988 (Commonwealth)*, in relation to students' personal information obtained for the purposes of chapter 3 and 4 of the *Higher Education Support Act 2003 (Commonwealth)*. This includes compliance with the Notifiable Data Breach Scheme.

In the event of a Data Breach, the CIMT will refer to the Legal and Integrity team to ascertain if ECU is obligated to report the breach.

D. Insurance/Specialist Engagement

In the event of a Cyber incident, ECU will follow Unimutual's Cyber Protection Notification and Claims Protocol documented in **Appendix C**.

ECU's insurer also provides access to a panel of specialists that can be utilised by IT, even if a cyber claim is not accepted under ECU's cyber protection. In the case of a claim not being accepted, ECU covers the cost of the services provided (we have access to "lower than commercial market" panel rates). The Chief Information Officer is responsible for engaging when/if required.

The CIMT will notify ECU's Risk and Insurance Adviser in the event this occurs via email or phone (08) 6304 2824.

E. Work Health and Safety

As per the Work Health and Safety Act 2020, there are certain incidents that are notifiable to the regulator (namely Worksafe WA). The Work Health Safety and Wellbeing (WHS) team are responsible for the notification to the regulator. Therefore, if an incident is dangerous or includes serious injury or illness of a person, the WHS team must be included in the CIMT.

Refer **Appendix D** for a detailed list of incidents.

8. POST-INCIDENT REPORTING

Following a Critical Incident, a post incident review is to be conducted by the Strategic and Governance Services Centre (Enterprise Risk). A Major Incident may be subject to a post incident review if it is deemed that there are benefits from identifying lessons learned that may be applicable to the wider University.

The review is to be completed within a reasonable timeframe following the end of a Major or Critical incident and the post incident report should be submitted to the Recovery Director and the Risk and Incident Management Committee. Post incident reports for Critical Incidents will also be provided to the Quality, Audit and Risk Committee ('QARC').

9. RECOVERY

The Enterprise-Wide Business Continuity Plan (BCP) will be enacted to guide recovery efforts. The Enterprise-Wide BCP includes recovery protocols for a range of scenarios for the core functions of the University.

Please refer to the Critical Incident and Business Continuity Management Guidelines and the Enterprise-Wide BCP for further information on recovery.

APPENDIX A – CIMT MEETING AGENDA GUIDE

Meetings will usually be held via Microsoft Teams. Agenda outlines are detailed below.

Links to agendas are included on the CIMT Teams Channel under 'Files'

Agenda for 1st CIMT meeting is outlined below or accessible via Teams here: CIMT Agenda First Meeting

Objective: prioritise actions and confirm response team

1. Summary of incident (meeting convener)
2. Appointment of Recovery Director & Site Liaison (if applicable) for incident
3. Establish safety and security of students, staff, contractors involved in incident (Recovery Director)
4. Advice on initial media / communications strategy and approach (Corporate Communications)
5. Incident response actions (Recovery Director)
6. Consider whether there are any mandatory reporting obligations
7. Summary of actions
8. Confirmation of next meeting and attendees

Agenda for subsequent CIMT meetings is outlined below or accessible via Teams here: CIMT Agenda Subsequent Meetings

Objective: confirm incident response is on track towards recovery

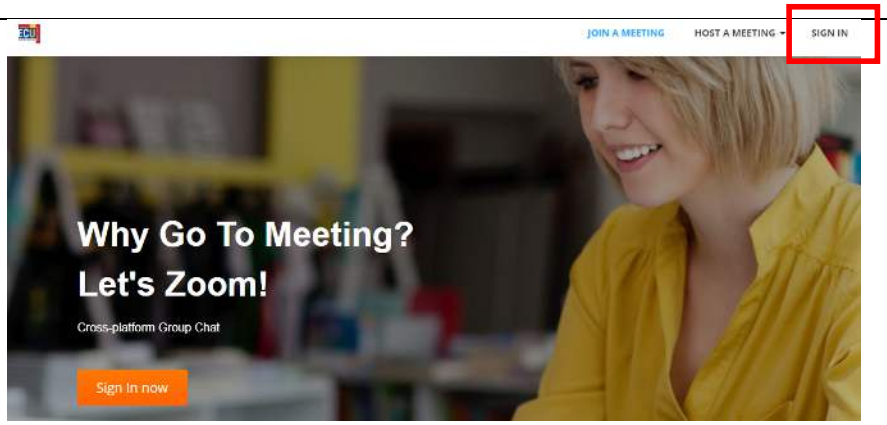
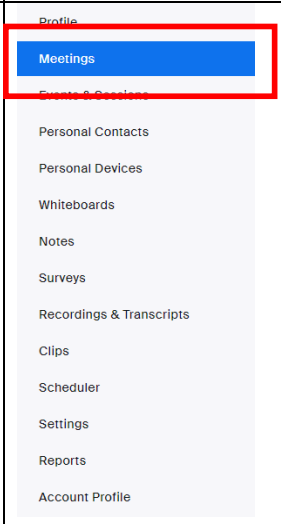
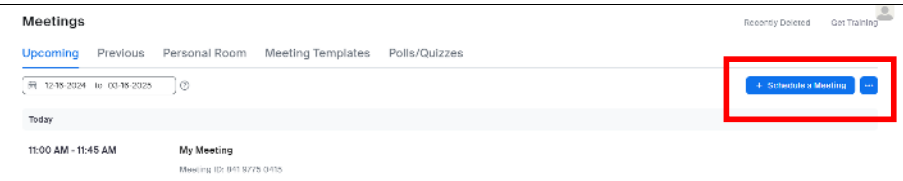
1. New information from Site Liaison and Recovery Director
2. Status of actions from previous meeting
3. Further communications/media actions
4. Summary of actions
5. Confirmation of next meeting and attendees

If Microsoft Teams is not available, the CIMT is to use Zoom to connect virtually – Refer Appendix B below.

APPENDIX B – SCHEDULING A MEETING VIA ZOOM (WHEN MS TEAMS IS UNAVAILABLE)

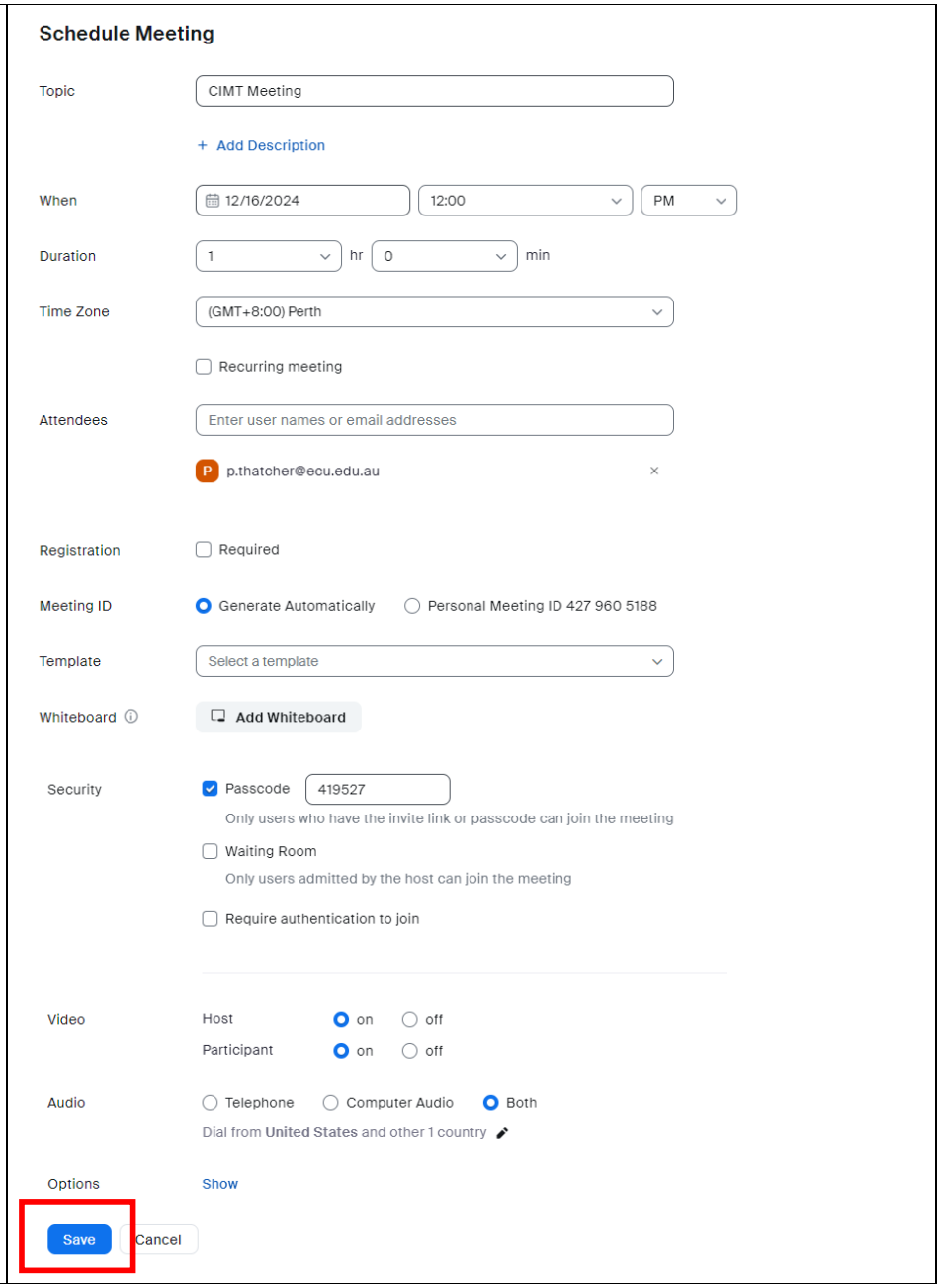
In the event that MS Teams is unavailable during a Critical Incident, Zoom should be used as an alternative mechanism for the CIMT to meet.

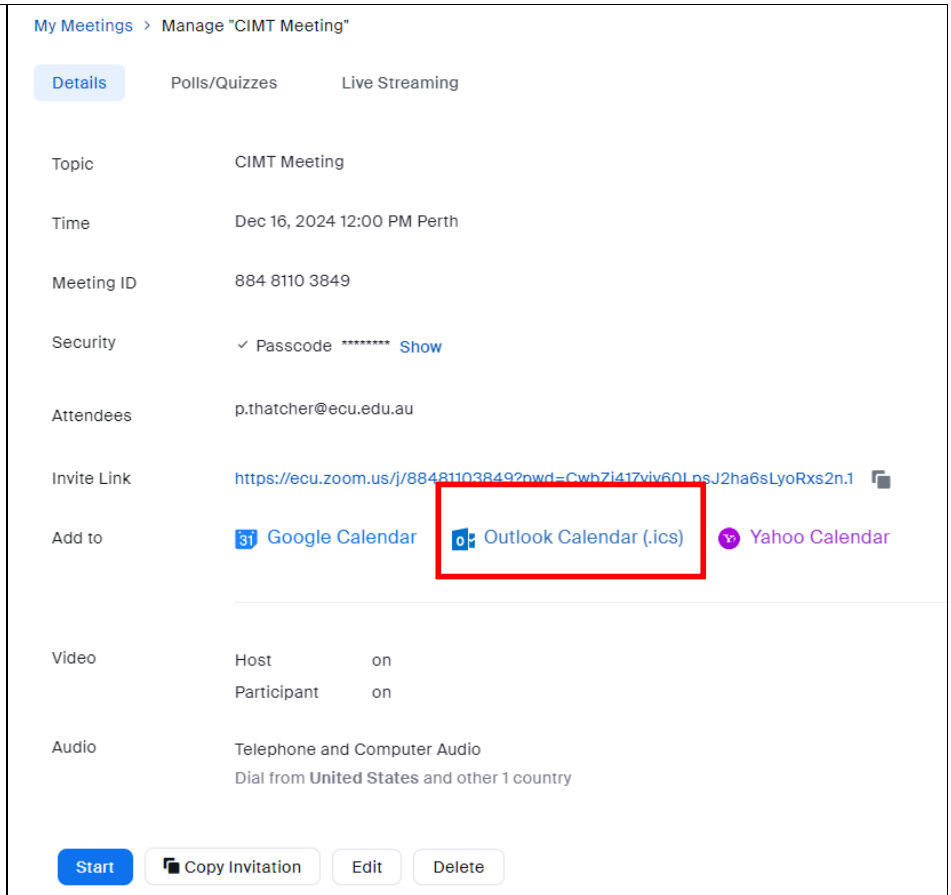
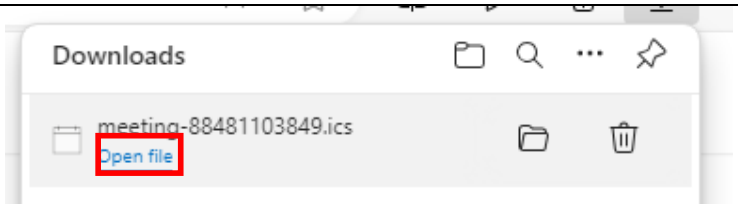
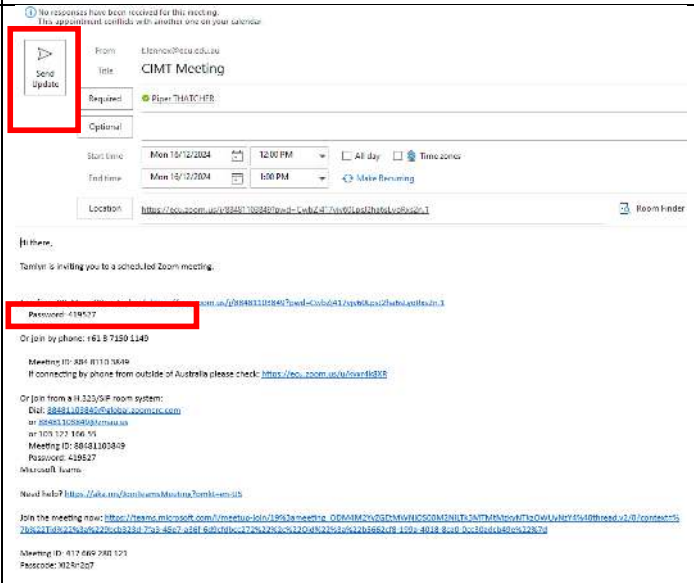
If you need to set up the Zoom meeting, take the following steps.

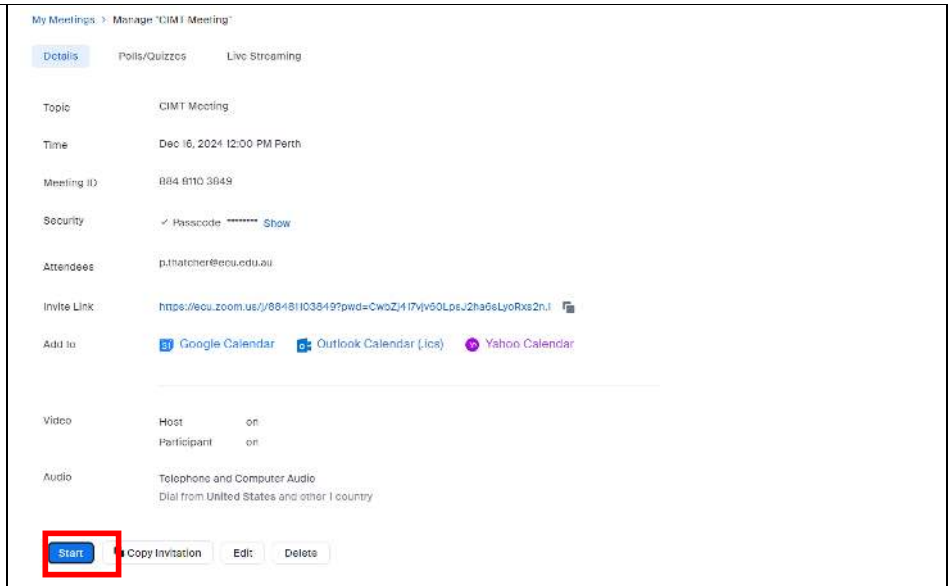
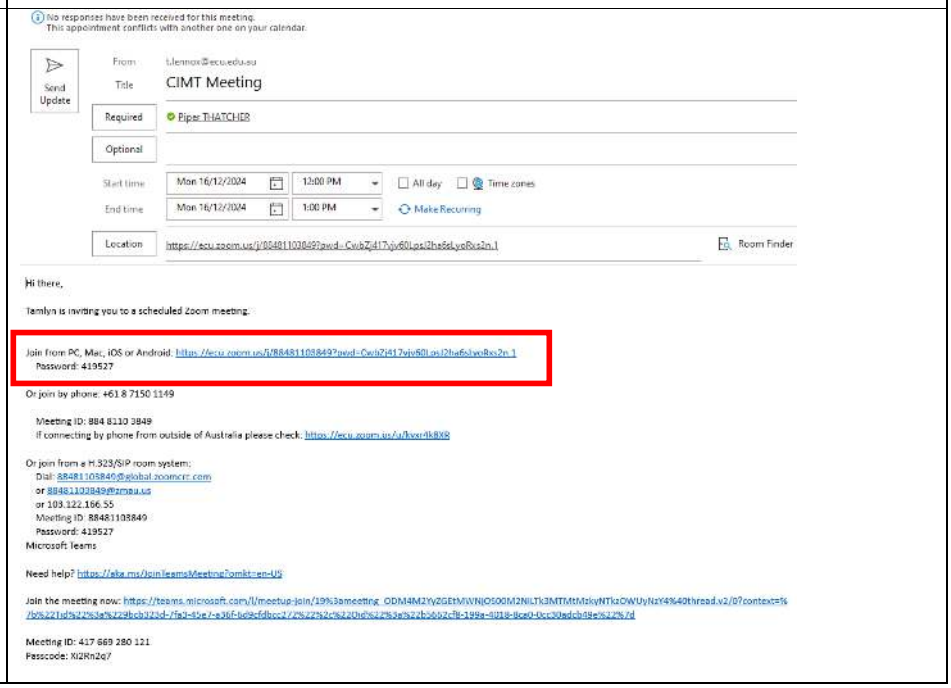
Steps	
1. Log into ECU's instance of Zoom via the following link: https://ecu.zoom.us/ Log in using your ECU username and password	
2. Select meetings	
3. Select Schedule a Meeting	

4. Schedule the meeting. This includes:

- Picking the date, time and duration
- Manually entering the email addresses of attendees
- Meeting ID: Generate automatically
- Security: Password
- Video: Host and Participant (On)
- Audio (Both)
- Hit Save



5. You will be taken to meeting details. Select Add to: Outlook Calendar	
6. The outlook calendar invite will be downloaded. Select open file.	
7. This will bring up the calendar invite. All invitees should already be noted as required – double check list is complete, highlight the 'password details' and then hit 'Send Update'	

8. If the meeting is due to start immediately, you can access the meeting by hitting the Start button below.	
Alternatively, if the meeting has been scheduled at a later time/date, you can access the Zoom meeting at the right time using the link in the email.	

APPENDIX C – CYBER PROTECTION: NOTIFICATION AND CLAIMS PROTOCOL

Cyber Protection

Notification and Claims Protocol

The Purpose of this document is to act as a guide for Universities and AXA XL to follow in the event of a Cyber Incident. It is not intended to and shall not form part of the Cyber Protection Policy. It identifies relevant key contacts, process and documentation required to expedite the claim and actions to be taken by relevant parties.

If it is known, or there are reasonable grounds to suspect, that you suffered a *Data Breach, Network Compromise or Extortion Threat,* a quick and effective response will help avoid or minimise exposure to lawsuits and regulatory inquiries.

Please call the AXA XL Data Breach team Hotline on **1800 466 380** which is monitored 24 hours per day, seven (7) days a week by our selected *Breach Response Provider, Crawford & Company.*

When the call is placed please have the following information available:

- Caller Information
  - Preferred language
  - Caller's First and Surname
  - Primary and Secondary Phone numbers
  - Email Address
  - Company Name
  - Country
- Incident Date/Time
- Incident Location (Address incl. City and Country)
- Incident details
  - Incident Details (Please provide information and background about discovery of the incident, type of incident, any steps taken to mitigate the effects of the incidence, persons affected etc.)
  - If data breach, type of data (Medical, Financial, Personally Identifiable Information)
  - Is theft or fraud suspected?
  - Number of data records involved
  - Any additional information you consider relevant
  - Status of the incident

The Crawford team will you call back within 1 hour of the initial notification to discuss a Mitigation Response Plan. In conjunction with contacting the AXA XL Cyber Response Hotline, notice of claims and/or circumstances should also be made to **AXA XL** at: *NewClaimAUFinancialLines@axaxl.com* *and* **Unimutual** – Jamie Thomson at: claims@unimutual.com.au

One of our AXA XL Cyber Claims team members will contact you to discuss the preliminary Mitigation Response Plan put in place by Crawford and the steps taken which may include:

- Briefing on background and status of the incident
- Immediate steps to be taken by you
- Coordination of your internal key contacts
- Discussion on potential third party vendor required
- IT Security and forensic computer vendor
- Public Relations or Crisis Communications vendor
- Policy response

AXA XL will work together with you and Crawford to execute your Mitigation Response Plan and carry out a preliminary assessment of seriousness and risk of harm. If necessary, we will coordinate notification to regulators law enforcement bodies, affected customers and other third parties.

Unimutual Limited Suite 11.02, Level 11, 56 Pitt Street, Sydney NSW 2000 | PO Box H96, Australia Square NSW 1215
T: 02 9247 7333 | F: 02 9252 9070 | service@unimutual.com.au | www.unimutual.com
Unimutual Limited ABN: 45 106 564 372 AFS Licence No: 241142

APPENDIX D – WORK HEALTH AND SAFETY CONSIDERATIONS

As per the Work Health and Safety Act 2020, there are certain incidents that are notifiable to the regulator (namely Worksafe WA). The Work Health Safety and Wellbeing team are responsible for the notification to the regulator. Therefore, if an incident includes any of the below, the WHS team must be included in the CIMT.

Requirement

notifiable incident means – the death of a person; or

a serious injury or illness of a person:

a) that requires the person to have immediate treatment as an in-patient in a hospital; or
b) that requires the person to have immediate treatment for —
    i. the amputation of any part of the person's body; or
    ii. a serious head injury; or
    iii. a serious eye injury; or
    iv. a serious burn; or
    v. the separation of the person's skin from an underlying tissue (such as degloving or scalping); or
    vi. a spinal injury; or
    vii. the loss of a bodily function; or
    viii. serious lacerations; or
c) that requires the person to have treatment by a medical practitioner within 48 hours of exposure to a substance; or
d) that occurs in a remote location and requires the person to be transferred urgently to a medical facility for treatment; or
e) that, in the opinion of a medical practitioner, is likely to prevent the person from being able to do the person's normal work for at least 10 days after the day on which the injury or illness occurs, and includes any other injury or illness prescribed by the regulations but does not include an illness or injury of a prescribed kind.
f) any infection caused by work or related to doing work that includes:
    i. working with microorganisms
    ii. the provision of treatment or care to a person
    iii. contact with human blood or body substances
    iv. handling or contact with animals, animal hides, skins, wool or hair, animal carcasses or animal waste products
g) any zoonoses (infectious diseases that can pass from animals to humans) that are contracted in the course of work that involve handling or contact with animals, animal hides, skins, wool or hair, animal carcasses or animal waste products. Examples to watch out for include:
    i. Q fever
    ii. anthrax
    iii. leptospirosis
    iv. brucellosis
    v. hendra virus
    vi. avian influenza
    vii. psittacosis
h) psychological injuries where they meet the above criteria and where they are a result of sexual assault or sexual harassment.

a dangerous incident:

means any incident at a workplace that exposes any person to a serious risk resulting from an immediate or imminent exposure to —

a) an uncontrolled escape, spillage or leakage of a substance; or
b) an uncontrolled implosion, explosion or fire; or
c) an uncontrolled escape of gas or steam; or
d) an uncontrolled escape of a pressurised substance; or

e) the fall or release from a height of any plant, substance or thing; or
f) the collapse, overturning, failure or malfunction of, or damage to, any plant that is required to be design or item registered under the WHS regulations (e.g. a collapsing crane); or
g) the collapse or partial collapse of a structure; or
h) the collapse or failure of an excavation or of any shoring supporting an excavation; or
i) the inrush of water, mud or gas in workings, in an underground excavation or tunnel; or
j) the interruption of the main system of ventilation in an underground excavation or tunnel;
k) electric shock that must be notified; or
l) minor shock resulting from direct contact with exposed live electrical parts (other than low voltage) including shock from capacitive discharge
m) electric shock that does not require notification:
    i. shock due to static electricity
    ii. extra low voltage shock (i.e. arising from electrical equipment less than or equal to 120 VDC)
    iii. defibrillators used to deliberately shock a person for first aid or medical reasons

<u>dangerous goods:</u>

any incident involving dangerous goods incident where people, property or environment are harmed must be reported. An incident involving dangerous goods must also be reported if:

a) but for intervening events, it could have resulted in unreasonable (i.e. serious) harm to people, environment or property (i.e. near miss or hit)
b) it results in a dangerous situation
c) it is specified in the dangerous goods safety regulations.

APPENDIX E – CRISIS COMMUNICATIONS MATRIX

Audience	Deliverable	Channels	Frequency	Who?
Staff	Informational updates from Recovery Director Overarching / inspiring message from VC at beginning, end of crisis	Global email Staff portal FAQs	Initial, then daily/as needed	Chief People Officer, Corporate Relations
Staff – researchers	Research-specific contingencies, information	Email FAQs MS Teams	Immediate, then as needed	DVC (Research)
Staff – T&L	Teaching-specific contingencies, information	Email FAQs MS Teams	Immediate, then as needed	DVC (Education)
Staff – Commercial services	Informational updates	Email FAQs MS Teams	Immediate, then as needed	VP Corporate Services
Students – all	Informational updates from DVC(E) / Director Student Life Overarching message from VC at beginning, end of crisis	Global email SMS Social Student Portal FAQs	Immediate, then as needed	Corporate Relations Student Life Growth, Engagement and Marketing
Students – HDR	Research-specific contingencies, information	Email FAQs	Immediate, then as needed	Graduate Research
Students – International	For issues affecting international borders, visas, enrolments etc.	Email FAQs	As needed	Student Life/ International Office
Students – Future	Providing holding lines/FAQs to address enquiries	FAQs	Initial, then as needed	Corporate Relations
Chancellor / Council	Updates on staff, student communications and issues management	Email	As needed	Strategic & Governance Services
Media	Holding statement Media release	Email	As needed	Corporate Relations
Alumni	Rescheduled events	Email Social	As needed	Development and Alumni Relations

APPENDIX F – CIMT CORE TEAMS

The CIMT is outlined in Section 4. Depending on the type of incident, the CIMT may not require all participants, or may require additional participants. The table below sets out the suggested CIMT for each incident type:

Property / Facilities	**Information Technology / Cyber**
• Vice-President (Corporate Services) • Director, Campus Environments • Chief Information Officer • Manager, Campus Operations & Support • Manager, Buildings and Planning • Manager, Corporate Communications • Chief Risk Officer	• Vice-President (Corporate Services) • Chief Information Officer • Manager, Information Security & Governance • Manager, Customer Services • Director, Strategic & Governance Services • Manager, Corporate Communications • Chief Risk Officer
Student-specific	**Other (e.g. staff)**
• Deputy Vice-Chancellor (Education) / Deputy Vice-Chancellor (Students, Equity and Indigenous) • Executive Dean of affected School • Director, Student Life • Manager, Student Incidents & Support • Director, Strategic & Governance Services • Manager, Corporate Communications • Chief Risk Officer • Note the *Student Significant Incident Response Procedure*, owned and maintained by Student Life, provides additional guidance around process and protocols to be followed in the management of student related incidents.	• Vice-President (Corporate Services) / Deputy Vice-Chancellor (Students, Equity and Indigenous) • Executive Dean / Director of affected School / Centre • Chief People Officer • Chief Safety Officer • Director, Strategic & Governance Services • Manager, Corporate Communications • Chief Risk Officer
Potential External Agencies	
• Department of Fire and Emergency Services (DFES) • Western Australia Police (WAPOL)	

Other areas within the University may also be called upon to provide advice and guidance, dependant of the type of incident. These areas include:

- Work Health and Safety. The Work Health Safety and Wellbeing team must be included in the Critical Incident Management Team if the critical incident:
    - Applies to any item listed in Appendix C;
    - There are actual or potential Health and Safety consequences.

  For assistance with reporting an incident in Riskware, see the Incident Reporting and Investigation Guidelines, or contact the Work Health Safety and Wellbeing team.
- Legal and Integrity (where legal and/or compliance advice is required)
- International Office (for overseas locations and/or incidents on study tours, etc.)
- Finance and Business Services Centre;
- Library Services Centre
- ECU Communications Centre; and/or
- Schools

If an incident occurs at the Mount Lawley or South West campus, the CIMT will appoint a liaison to coordinate any support requirements. These liaisons would be:

Mount Lawley Campus	South West (Bunbury) Campus
• A member of the Senior Leadership Team based at the Mount Lawley campus; or • The Digital Services/Campus Environments representative.	• The Dean of the South West campus; or • The Digital Services/Campus Environments representative.