UNIVERSITY OF SUSSEX

Business Continuity Plan
Web Version – Draft - V1.0

Foreword

This Business Continuity Plan provides procedures and guidance for the management of disruptive incidents, which may adversely affect services and activities at the University of Sussex.

The intention of this plan is to ensure that the University will have the capability to continue its highest priority activities, to an acceptable level during and after disruptive incidents.

Should the University be affected by disruption, Schools and Services will be expected to introduce pre-planned contingency arrangements, in order to facilitate education and critical research in challenging circumstances. In addition, the University will be expected (as far as is practicable) to continue to provide suitable accommodation, catering facilities, cleansing and welfare services, when faced with a disruptive incident.

This plan will provide a framework to enable the University's management to oversee the response to and recovery from a disruptive incident, with particular attention given to the highest priority activities.

This plan will align with the University's approved command and control arrangements when responding to (and recovering from) such incidents as defined in the Incident Response Protocol. Within this context, it is acknowledged that decision making may be undertaken by incident commanders outside of the University's normal governance and reporting processes, in order to support a timely response to associated risks and issues as they arise. Key decisions will be recorded in the incident log and reviewed during the de-brief process.

The University's Schools and Professional Service Divisions are expected to prepare for incidents by assessing the potential impact of disruption and maintaining local plans to respond to incidents. These plans may involve temporarily suspending certain activities in order to maintain essential services to acceptable levels. Those Schools and Divisions with responsibilities for higher risk or business critical activities will prepare specific plans to deal with interruptions, so as to enable resumption and recovery to commence within an acceptable period of time.

Heads of Schools and Professional Services Directors and their leadership teams will be consulted throughout the business continuity planning process and the University will liaise with external partners and key stakeholders when necessary.

This plan will be reviewed annually by the General Counsel with oversight from the University Executive Group.

Business Continuity Management - Policy Statement

Business continuity can be defined as "The capability of an organisation to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident". (BCI Good Practice Guidelines 2018)

The aim of the University's Business Continuity Management (BCM) Programme is to identify the main threats, which have the potential to disrupt priority activities and to develop measures which protect against interruptions, facilitate a response to incidents and support recovery.

The objectives of the University's BCM Programme are to:

- Improve resilience within the University's people, assets, systems and infrastructure
- Develop contingency arrangements that are safe and secure for all personnel
- Facilitate the co-ordinated recovery of priority activities
- Support incident response and recovery with effective communications

By implementing the BCM programme, the University will be better prepared to effect a coordinated response to disruptive incidents

The University's Schools and Professional Services will be expected to identify potential threats to their operations, examine the impact of disruption and make local plans for responding to incidents in order to improve resilience. The University's approach to procurement aims to ensure that such standards are expected where services are provided by contractors or third party suppliers.

All staff are expected to recognise and detect the risk of disruption to the core activities of their School or Division and report any concerns to management. Managers are expected to evaluate these risks, design and maintain business continuity plans to cope with disruption and agree response and recovery procedures with service providers and all team members.

These arrangements may involve certain staff performing temporary roles, at different times or in alternative locations. During disruptive incidents, staff may be asked to consider such changes to their normal working arrangements, to support the University throughout the recovery process. The University will ensure that any proposed alternative working arrangements are safe, suitable and secure.

By reviewing and maintaining these arrangements and learning from incidents, the University will strive to continually improve resilience across the institution, which should serve to reduce the impact of disruptive incidents.

The intention is for business continuity planning to become embedded in to the routine management activities that take place within the University's Schools and Professional Services.

Contents

PART 1 – Business Continuity Plan – (Strategic & Tactical)

PART 2 – Business Continuity Plan - (Operational)

List of Appendices

Record of Amendments

Amendment Number	Amended section (s)	Date
1	Revised Business Continuity Plan introduced	September 2018
2	Minor text edits	January 2019
3	Added additional information for BRGs	July 2019
4	Minor edits to reflect organisational change	April 2021
5	Emergency response information now included in BCP	April 2022
6		
7		
8		
9		
10		

1.0 INTRODUCTION

1.1 Background

Within any organisation, normal business can be disrupted at any time. These disruptions can be caused by:

the loss of personnel – e.g. due to illness or industrial action
the loss of access to facilities, equipment or premises – e.g. due to fire or severe weather
the loss of infrastructure – e.g. power outage, IT failure, cyber-attack or fuel shortage
an interruption to the supply chain – due to any of the above or other external influence which affects suppliers

Those responsible should therefore prepare for disruption by identifying where their activities may be vulnerable, by assessing the likelihood and impact of interruptions and devising and documenting 'local' plans to respond and recover to incidents effectively.

The University of Sussex is a leading higher education and research institution situated in the city of Brighton and Hove. The majority of activities are centred on the University's Falmer Campus, which boasts award-winning architecture and is situated in the beautiful South Downs National Park.

The University has twelve Schools providing education and research opportunities to more than 19,000 students, approximately 5,000 of whom live on Campus. More than 3000 staff are employed within the University's Schools and Professional Services to deliver high quality education and research programmes and providing an excellent student experience.

The following services are available 24/7:

- Security (York House)
- Campus and Residential Services (York House Reception and in each Hall of Residence)
- The University Library (during term-time)
- The Student Centre

In addition, specialist staff and senior management will be available to respond to urgent incidents, which may arise outside of normal office hours and/or away from the main campus.

The generic procedures within this Business Continuity Plan are intended to enable an effective and co-ordinated response to a disruptive incident involving the University's activities, premises, students, staff, contractors or suppliers.

Heads of Schools and Professional Services Directors are required to formulate and maintain specific emergency and business continuity plans so that they can effectively initiate the response to 'local' incidents. These plans should contain the details of all staff, contractors, resources and suppliers who are critical to service delivery and procedures to define the local management arrangements for responding to incidents and to cope with disruption to their normal operations, with specific contingency arrangements to protect their priority activities. Duplicates of essential materials, equipment and data should be stored in a secure, alternative location. Alternative working arrangements (e.g. remote working and service delivery) should also be considered as part of these plans, where applicable.

A Business Continuity Plan Template is provided in Part 2 of this document. Those responsible for preparing BC Plans should also refer to the following documents:

<table>
<tr><td rowspan="2">UoS Incident Response Guidance</td><td>UoS Incident Contacts Directory</td><td rowspan="2">Sussex Community Risk Information</td></tr>
<tr><td>UoS Crisis Communications Plan</td></tr>
</table>

1.2 Aim of the Business Continuity Plan

The aim of this Business Continuity Plan is to enable University staff to prepare for disruption and make informed decisions, which support the continuity of priority activities during disruptive incidents.

1.3 Objectives

The objectives of this Business Continuity Plan are to provide a framework for incident managers which will enable them to prepare for disruption and:

- Respond to disruptive incidents and enable the University to cope with their impact
- Facilitate the co-ordinated recovery of priority activities
- Continue to provide essential services, whilst giving priority to the most critical activities
- Develop alternative arrangements that are safe and secure for all personnel

1.4 Scope

This plan provides a framework to enable senior management to deploy resources which support business continuity at the University of Sussex during the response to (and recovery from) disruptive incidents, as outlined in the University's Incident Management Guidance document.

Part 1 of this plan contains the procedures for the strategic management of disruption and Part 2 contains a template to assist the University's Schools and Professional Services in preparing specific local (tactical and operational) business continuity plans. During a major incident, the procedures within this plan aim to align with those specified within School/Divisional emergency/BC response and recovery plans.

1.5 Assumptions

In the formulation of this plan, it is assumed that the Heads of Schools and Professional Services Directors have examined the risk of disruption to their priority activities and that contingency arrangements have been identified, agreed, documented and shared in their local Emergency and BC Plans.

With support from the Senior Risk and Resilience Manager, Heads of Schools and Professional Services Directors will undertake a Business Impact Analysis to examine how disruption could affect the fulfilment of strategic objectives, compliance with statutory obligations or potentially damage the University's reputation and financial performance. Information from these BIA's will be collated by the Senior Risk and Resilience Manager and key activities (critical functions) will be given strategic priority for recovery based on the information provided. This process will be overseen by the General Counsel.

For this plan to be invoked, it is assumed that an incident is likely to interrupt the University's activities for more than one working day and that a normal operational response undertaken by the affected Schools and/or Professional Services will be insufficient to enable recovery in the required time. Higher risk activities may require a more urgent response and will be subject to specific plans, which will be owned by the relevant School/Division. Where staff shortages are referred to, the assumption is that at least a 50% reduction in normal staffing levels will be experienced and that this will have a noticeable impact on the education, research and the student experience at the University of Sussex.

1.6 Distribution

An electronic version of this plan is available on the University website.

1.7 Audit & Review

These business continuity arrangements are subject to periodic inspection by the University's internal auditors and will also be shared with the University's insurers. The Senior Risk & Resilience Manager will review the BC Plan annually and the General Counsel will notify the Chief Operating Officer of any significant amendments. Updates may be issued in the light of any disruptive incidents, changes to the University's governance, structure, priorities or activities, or following any major alterations to the Campus environment.

1.8 Training & Exercising

The Senior Risk and Resilience Manager will develop a programme to raise awareness about Business Continuity within the institution and will work with members of the University's Risk and Resilience Management Group (RRMG) to deliver training and exercises in this regard. The University's Leadership Team will be briefed on the contents of this plan and best practice approaches to BCM. Heads of Schools and Professional Services Directors will be expected to brief their teams about the importance of business continuity to the University and its objectives.

The Senior Risk and Resilience Manager will be responsible for exercising the University's business continuity arrangements in consultation with the Risk and Resilience Management Group. In the absence of a disruptive incident, it is recommended that Schools and Professional Services review their local emergency and BC arrangements at least once a year and this can be done during routine departmental meetings.

Following an exercise or disruptive incident, the relevant Head of School or Professional Services Director will produce a de-brief report to identify any lessons and inform any future arrangements, in order to improve resilience.

1.9 Types of Disruptive Incident

1.9.1 Critical Incident – interruption which affects a small number of non-critical activities for a short period of time. Examples include single room failure, short-term outage and small-scale, short-term evacuation. Critical incidents are expected to be managed with a local response by the affected Schools or Services, although assistance may be sought from other teams such as SEF Support Services, Security or Estates as part of their normal operations.

1.9.2 Significant Incident – disruption to core activities, the impact of which will be noticed by the University community, on campus or elsewhere. Examples include a short duration IT or utility outage or a severe weather event which causes hazardous conditions on campus. Significant incidents are likely require specialist advice, additional resources, communications planning and tactical co-ordination to support response and recovery efforts.

1.9.3 Major Incident – prolonged disruption to critical activities which may affect the University's objectives. Examples include the loss of (or severe damage to) a University building or other major asset, a large scale evacuation, a prolonged cyber-attack, or an outbreak of a life-threatening infectious disease. Such incidents will require strategic management, crisis communications and close liaison with external partners to support recovery.

1.10 Risk Assessment – Possible Causes of Disruption

The Sussex Community Risk Register identifies the main local hazards and threats. In business continuity terms, the University's top risks can be categorised as follows:

Threat	Implication for 'Business as Usual'
Pandemic Illness	Staff shortages, mass vaccination, social distancing, anxiety
Industrial Action	Availability of staff and contractors
Severe Weather	Hazardous conditions, utility failure, staff shortages
Denial of Access to a Building	Hazard, blockade or outage restricts access
Protests & Disruptive Events	Access, safety and security on campus
Utility failure	Loss of power/water/heating
Cyber-attack/IT outage	Systems down, service disruption, compromise of data
Local Major Incident	Evacuation or denial of access to facilities

IMPACT						
	5. Severe **Disruption** **> 1 month**			Damage to or loss of facilities (e.g. due to fire or flood)	Pandemic Illness Prolonged Industrial Action	
	4.Major **Disruption** **< 1 month**			Campus Pollution Incident	Prolonged IT or Utilities Outage Cyber Attack	Denial of Access to a Key Asset
	3. Significant **Disruption** **< 1 week**			Prolonged Supply Chain Disruption	Local Major Incident Data Breach	Severe Weather Protests & Disruptive Events
	2. Moderate **Disruption** **< 2 days**				Local 'Critical' Terror Threat	Welfare Incident Maintenance Defect
	1. Minor **Disruption** **< 4 hours**					Short-term Evacuation Short-term Outage
		1. Negligible **0.005%** **1:20,000**	**2. Low** **0.05%** **1:2000**	**3. Medium** **0.5%** **1:200**	**4. Moderate** **5%** **1:20**	**5. High** **50%** **1:2**

LIKELIHOOD OF OCCURRENCE IN c5 YEAR PERIOD

Risk Rating Key		
Low	Business as usual	
Medium	Monitored locally & managed by operational plans	
High	Prepare and maintain BC Plans to mitigate	
Very High	Priority for attention, specific plans may be required	

1.11 Business Impact Analysis (BIA)

The Business Impact Analysis (BIA) forms a key part of the Business Continuity planning process. Heads of Schools and Professional Services are expected to undertake a BIA to identify their priority activities and examine the impact of disruption on them, over time. The impact of such interruptions will be assessed according to the University's:

- People
- Reputation
- Financial performance
- Operations
- Statutory compliance

Information from the Business Impact Analysis will be used to identify activities to be given strategic priority for resumption and recovery following a disruptive incident. The BIA should also inform decision making as to which activities could be temporarily suspended to allow the most critical functions to continue or resume operations during and after disruptive incidents.

1.11.2 Priority Activities

The prioritisation of activities, processes and resources will be described as follows:

- **Priority 1**: Essential activities requiring urgent resumption and recovery within 24 hours to safeguard the University's reputation and strategic objectives. These activities should have specific, adequately resourced incident response plans and clearly defined contingency arrangements, which will be owned by the Head of School or Professional Service Director and approved by the Provost or Chief Operating Officer.

- **Priority 2**: Activities requiring resumption and recovery to commence within 48 hours in order to resume essential University services and maintain performance. Local BC plans will be approved by the Head of School or Professional Service Director, who will be responsible for invocation, to coordinate the required response.

- **Priority 3**: Activities with a recovery time objective of more than 48 hours. Whilst the impact of disruption upon activities may not be immediately noticeable, productivity and performance may continue to decline over time, which will negatively impact objectives. A backlog of incomplete tasks may accumulate as a result of reduced operating capacity and/or resources being allocated to the recovery process. Therefore, local (team level) BC plans should be developed and maintained by the relevant Coordinator or Head of Department and approved by the School/Divisional Management Team.

- **Priority 4**: Non-essential activities which may be suspended indefinitely to support any of the above with negligible impact on the University's objectives.

Priority 1 and 2 activities will be examined and ranked during the BIA process and specific, local contingency plans will be developed by the risk owners and shared among the relevant teams.

Priority 3 and 4 activities will be considered in local BC planning processes, so as to identify and agree suitable alternative working arrangements.

1.12 Dependencies

During the Business Continuity planning process, Schools and Professional Services will be required to identify and note their key dependencies on other services, such as those provided by ITS or Estates, as well as contractors or suppliers. Where such dependencies exist, procedures for responding to incidents should be pre-agreed, specified in BC plans and given due consideration when setting business continuity objectives.

1.13 Vulnerability

The University is heavily reliant on the availability of more than ninety buildings and associated infrastructure operating from its Falmer Campus. This includes the operation of:

- accommodation for more than 5000 students
- teaching and study spaces such as lecture theatres, seminar rooms and the Library for c19000 students
- controlled research areas e.g. laboratories containing hazardous equipment, unique materials or animals
- offices, meeting rooms and specialist work spaces for staff and tenants
- catering and retail outlets
- the ACCA, sports facilities and the Meeting House
- the Medical Centre, Pharmacy and Nursery
- the wider campus estate, including the road/footpath networks and car parks

The Campus is situated within the Southdown's National Park. Given its topography and built environment, certain areas of the Campus are susceptible to surface water flooding, following heavy rainfall. Many of the buildings are flat-rooved and are vulnerable to water ingress, particularly when guttering and drainage systems become blocked or overwhelmed following heavy rainfall.

Given the complexity surrounding the University's built environment, Schools and Professional Services are advised to report concerns regarding such vulnerability to Sussex Estates and Facilities (SEF) to ensure that critical activities are protected against the risk of flooding and that suitable contingency arrangements are in place to maintain essential services should an incident occur.

All of the major transport and pedestrian routes access the site via its southern boundary. This complicates access arrangements for emergency services vehicles and limits the opportunities for evacuation. In addition, any external incident leading to the closure of one of the local major transport routes would have the potential to cause significant disruption to the University's activities. This also limits the evacuation routes from campus.

Utilities on Campus (e.g. power, water, gas) may occasionally be interrupted and the initial response to such incidents will be facilitated by the Estates Division, in conjunction with SEF. Schools and Services requiring a constant utility supply (e.g. to support priority activities, critical systems or vital research materials and equipment) should make specific local plans to ensure that auxiliary supplies are available and operational when required.

Schools and Professional Services are heavily dependent on IT systems and network connectivity to deliver education and research programmes and support the student experience. The availability of IT systems is particularly important during peak times such as clearing, confirmation, registration and enrolment and also around assessment submission dates. Therefore, Schools and Professional Services should form specific, co-ordinated plans to respond to IT disruption and communicate effectively. The ITS Disaster Recovery Plan specifies the procedures and timelines for recovery in the unlikely event of a prolonged outage to the University's IT systems.

Protests and demonstrations occasionally occur on the University campus and these have the potential to disrupt education, research, support services and campus operations. Buildings such as Sussex House have been subject to blockades and occupations which can last for several days. Owing to this particular risk of disruption, a specific BC Plan for Industrial Action, Protests and Demonstrations has been prepared and shared with the relevant staff.

2.0 ACTIVATION, MANAGEMENT & COORDINATION

2.1 Activation - This plan will be activated in the following circumstances:

a) A sudden onset incident which interrupts critical activities or causes significant disruption to the University for at least one working day.

Initial Action:

- If necessary, SEF staff will coordinate the evacuation and security of the affected part(s) of Campus, in accordance with their emergency response procedures.
- If the incident is disrupting key computer systems, IT Services will invoke their Disaster Recovery and Service Continuity Plans and inform the relevant Schools and Divisions.
- If strategic management is required, the University Incident Management Team (UIMT) will be alerted, so that they can assess the situation and provide a statement of intended action (See Appendix 1 and 2).
- UIMT will invoke this plan if the incident is likely to cause significant disruption to students, staff or priority activities.

b) A foreseen incident which interrupts urgent activities or causes significant disruption to the University for at least one working day.

Initial Action:

- Advance planning and risk assessment – Heads of Schools and Professional Services Directors will assess the likely impact and consider the need to invoke local pre-prepared BC plans, which will define preparatory activities and contain pre-agreed alternative working arrangements and the communications strategy.
- When severe weather is expected, EFM/SEF will co-ordinate the University's preparedness and response activities and maintain the necessary documentation, such as the University's Severe Weather Plan.
- If prolonged industrial action is likely to disrupt priority activities, HR will take the lead in assessing the risk, issuing communications and initiating the University's preparatory and response activities, as defined in the University's BC Plan for Industrial Action.
- If strategic management is required, UIMT will be alerted to assess the situation, provide a statement of intended action and arrange for it to be communicated. (See Appendix 1 and 2)
- Heads of Schools and Professional Services Directors will report concerns to UIMT and identify priorities for support.

2.2 Notification

The majority of emergency incidents will be reported to Security by dialling 3333 (01273 873333). The Security Control Room operates 24/7. Upon notification of an incident, Security will assign a Site Incident Manager to oversee the initial response. Estates maintenance and utilities emergencies (where there is no immediate threat to life) should be reported to the SEF Service Centre on 7777 (01273 877777). IT outages should initially be reported to the IT Services Helpdesk 8090 (01273 678090). Incidents may also be reported from elsewhere (e.g. from those studying abroad). The escalation can call-out process is described in the University's Incident Response Guidance document.

Where there is likely to be media interest and the potential for reputational damage to the University, the incident commander will notify the Director of CMA, in accordance with the University's Crisis Communications Plan.

Heads of Schools and Professional Services Directors will be responsible for notifying personnel from within their teams and maintaining local contacts lists to facilitate this. In addition, the relevant Head of School/Professional Service Director will determine when it is necessary to notify the University Incident Management Team about a local incident that may have a University-wide impact.

The **University Incident Contacts Directory** contains the personal contact details for alerting all members of UIMT should escalation be necessary, as well as other incident responders, local partners and stakeholders for external engagement.

2.3 Incident Management - Command & Control

2.3.1 Incident Response & Recovery Teams (IRRT) – BRONZE Command

In many cases, response and recovery may be managed by specialist local teams invoking their specific local Emergency/Business Continuity Plans. A sample Business Continuity Plan template is available in Part 2 of this document.

Incident Response and Recovery Teams (IRRTs) will facilitate the operational response to emergencies and other disruptive incidents within Schools and Professional Services.

The priorities will be to:

- Ensure the safety of all personnel who are affected by (or responding to) the incident
- Capture and record information about the incident
- Notify and liaise with other relevant schools and departments
- Invoke specific local BC plans as appropriate
- Adopt pre-agreed, alternative ways of working to support the continuity of priority activities
- Escalate to Silver Command if additional resources are required to manage the disruption

2.3.2 Local Incident Management Teams (LIMT) – SILVER Command

IRRT Leaders will determine if there is a need for the tactical management of the response and recovery process**.** If this is the case, it may be necessary to escalate command of the incident to Local Incident Management Teams (LIMTs).

LIMTs will call upon expertise from within the relevant Schools and Professional Services Divisions to facilitate the tactical response to significant incidents**.** LIMTs may initially be clustered together to form the Campus Operations and Education and Students Groups, in order to prioritise BC and co-ordinate the response and recovery processes.

In BC terms, the priorities for LIMTs will be to:

- Protect people and assets.
- Coordinate the activities of any responding IRRTs.
- Determine the need to merge LIMTs into Campus Operations Group and Education and Students Group.
- Ensure that resources are targeted appropriately to support safety, wellbeing and the student experience.
- Provide accurate information to communicate about the incident.
- Notify the UIMT if strategic incident management is required.
- Co-operate and provide updates from local specialists in order for UIMT to make decisions.

2.3.3 University Incident Management Team – (UIMT) – GOLD Command

A large-scale, University-wide response by numerous LIMTs may need to be coordinated by the University Incident Management Team (UIMT). When prolonged disruption is expected**,** the Chief Operating Officer/Provost will decide whether to declare a major incident and convene a meeting of UIMT. Members of UIMT (identified in Section 5 of this document) will be on call to attend meetings out-of-hours as necessary.

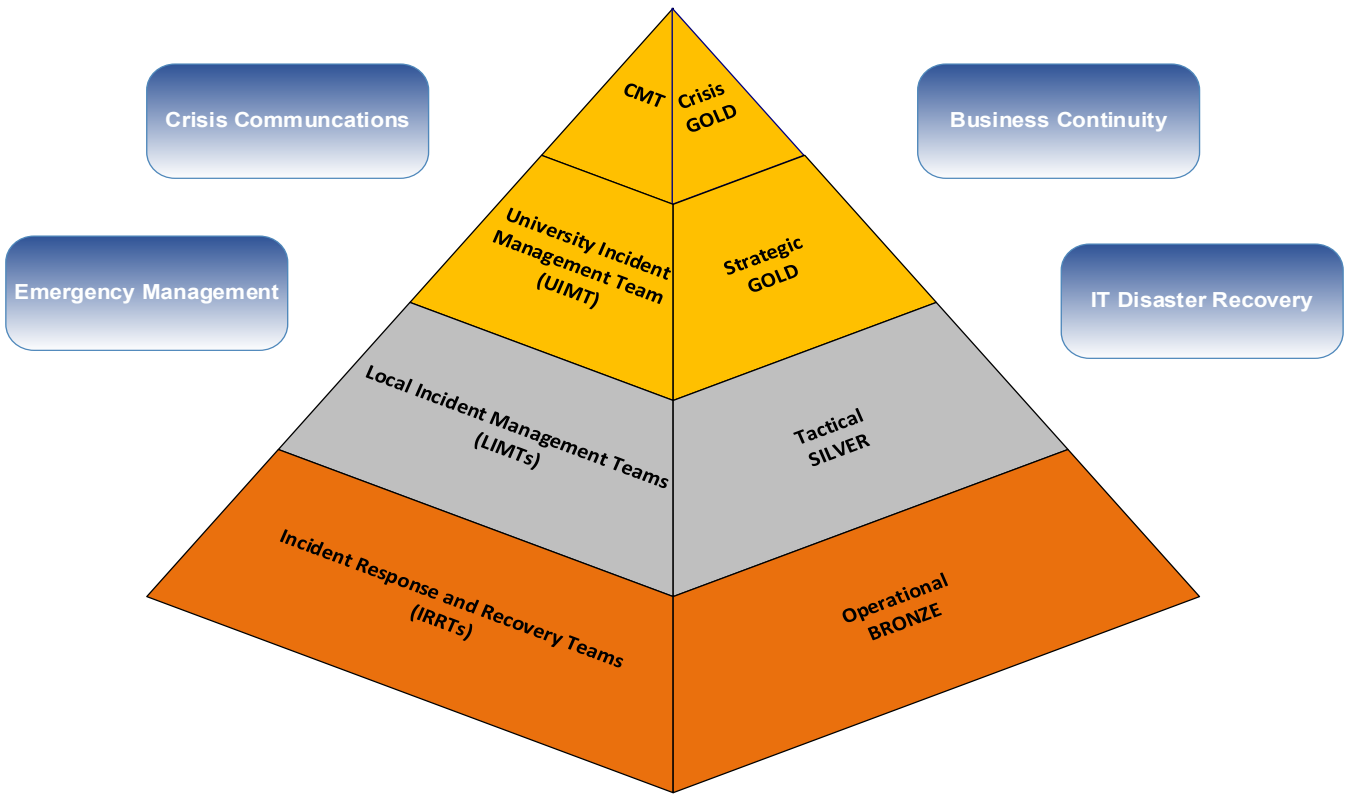
Meetings of UIMT may initially take place remotely, but if in-person meetings are required, they will take place in the Sussex House Committee Room (SH307/308). However, if Sussex House is not available, UIMT may convene at alternative locations such as Bramber House (Room 405), the Firle Room in the Hastings Building or at an off-site location to be agreed.

UIMT will assume the strategic management of a disruptive incident, which affects the University's priority activities. UIMT will examine the impact of the incident, identify immediate priorities and determine the strategy for recovery. UIMT will make key decisions to coordinate the response and recovery efforts and agree the internal and external communications strategy in line with the University's Crisis Communications Plan. A sample agenda for this first meeting is provided as Appendix 1 of this document.

In BC terms, the priorities for UIMT will be to:

- Make key decisions and coordinate the University's response to a Major Incident
- Determine the strategy for recovery
- Provide information and support to all stakeholders

University of Sussex Incident Response Structure



2.3.4 Crisis Management Team (CMT) (to assume GOLD Command if appropriate)

In the context of business continuity, a crisis can be defined as an unstable, irrational incident that creates a severe level of disruption. The impact of a crisis may exceed what could have reasonably been expected and therefore may not have otherwise been planned for. In these circumstances, the University's Crisis Management Team will be required to provide strategic leadership and safeguard the University's priorities. The Vice Chancellor will Chair meetings of the CMT and will decide on who should attend. The UIMT Leader will be responsible for notifying the Vice Chancellor when an incident escalates to this level. The Vice Chancellor will act as the University's Gold Commander during these incidents and liaise with external partners and key stakeholders as necessary.

In BC terms, the priorities for CMT will be as follows:

- Acknowledge that a crisis has occurred and inform stakeholders and partners
- Monitor reports from IMTs and agree objectives to mitigate the impact
- Support financial sustainability and resilience
- Prepare and provide media statements to protect the University's reputation
- Monitor the fulfilment of the University's strategic priorities during recovery

2.4 Incident Control - Administration & Logging

Incident commanders should record all decisions, actions and the rationale behind them in an incident log. Schools or Services leading the response and recovery efforts will be expected to provide a member of staff to maintain this document. During a major incident, an Incident Control Room will be set up by the Risk and Resilience Senior Manager, if in-person meetings are required. Incident Control will monitor and share information to support decision making and deal with any unplanned issues as they arise. Incident Control can be contacted via email eim@sussex.ac.uk

2.5 Stand-down

Following an incident, Heads of Schools and Professional Services Directors will report to UIMT the time at which their service levels have returned to normal. This plan will be stood down when all affected Schools and Professional Services have confirmed that key activities are returning to normal levels.

Suggested protocol for Stand-down

1. Affected schools/services report a return to 'business as usual' operations
2. IRRT/LIMT de-brief
3. UIMT/CMT de-brief
4. Completion and return of decision logs and financial reports
5. UIMT/CMT announces that incident response and recovery are complete

2.6 De-brief

A de-brief should be held following any disruptive incident. The intention is to capture any learning to reduce the likelihood of the incident occurring again, control the impact and improve the capacity to recover. The incident de-brief should raise the following questions:

- what went well?
- what didn't go so well?
- what should be done differently in the future?
- have any gaps/vulnerabilities been identified which need to be addressed urgently?

3.0 Communication

3.1 Internal Communications

UIMT will require an initial situation report from LIMTs regarding the impact of the disruptive incident, how they are responding and the decisions that need to be taken**.** Students and staff will be updated based on what is known about the level of disruption, precautionary measures and working temporary arrangements in accordance with the University's Crisis Communications Plan, which is produced by the CMA Division. Messages will be broadcast by whatever means possible such as the University website, social media feeds, email and campus TV screens. Emergency alerts will be issued via the University of Sussex Mobile App.

3.2 External Communications

If there is interest from the local or national media, UIMT/CMT will agree an initial media statement, in accordance with the Crisis Communications Plan. The University's CMA Division will monitor media coverage of the incident and prepare responses accordingly. Information to external partners and stakeholders will be circulated by whatever means possible (e.g. website, press releases, social media etc.)

3.3 Incident Contacts

Each Local Incident Management Team (School/Division Level) is responsible for maintaining an up-to-date contacts list for staff, in order to notify them of an incident and to escalate to senior leaders, including out-of-hours.

The contact details of members of the University Incident Management Team (UIMT) will be held in the University's Incident Contacts Directory, which is an encrypted document. These contact details may be used out-of-hours, should the need arise.

3.4 Situation Reporting (SITREP)

Incident managers will use the Red, Amber, Green (RAG) reporting system to indicate the impact of the disruption on their service as described in the table below:

RAG Status	Disruption	Description of Impact	Response
Green	Minor	Short interruption (< 1 day) Local BC Plan invoked to support recovery Barely noticed by students or stakeholders	Normal Operations
Amber	Significant	Medium-term interruption (>1 day) Schools/services activities disrupted Local BC plans invoked to support recovery	Tactical Management
Red	Major	Prolonged interruption (> 2 days) Loss of facilities, equipment or personnel Critical activities suspended/prolonged recovery	Strategic Management

In the early stages of an incident, the full nature of the impact may be unclear. SITREPs should be statements of fact, providing an objective account of what has been confirmed as having happened, with a clear distinction between information which remains unconfirmed.

The adoption of this situation reporting system will ensure that the University's communications are aligned with external partners, such as the emergency responders.

4.0 Business Recovery

4.1 The Role of UIMT – to coordinate and provide a strategy for the recovery of the University's priority activities. To provide timely information about the incident to students, staff, stakeholders and external partners.

4.2 Business Recovery Groups

During the recovery phase of a major incident, UIMT may determine that LIMTs can be clustered into Business Recovery Groups, who will focus on shared priorities. Business Recovery Groups will be chaired by the relevant Professional Service Director and membership will include specialists from within their teams and representatives from the affected Schools/Divisions. See Appendix 3 for Business Recovery Groups' Initial Actions.

4.2.1 Personnel Recovery Group – Led by the Director of HR

Key Tasks - Oversee student and staff welfare during the recovery process
Ensure payments to staff are made on time
Advise on mitigation should Industrial Action disrupt critical activities
Liaison with USSU and relevant staff Trade Unions

4.2.2 Education and Research Recovery Group – Led by the Director for Student Experience, Relevant Heads of Schools and Director of Research & Enterprise

Key Tasks - Assessing the impact upon education and research activities
Initiate the assessment, salvage and recovery of damaged equipment and research materials
Providing wellbeing services to students and information about the incident and any disruption
Providing information about changes to timetabling, assessments, exams etc.

4.2.3 Estates & Facilities Recovery Group – Led by the Director of Estates and the Head of Service Delivery (Facilities Management)

Key Tasks – Securing the incident scene and engaging with the emergency services
Providing Health & Safety advice and assessing the environmental impact
Providing suitable emergency accommodation for displaced people
Identifying suitable sites for temporary buildings for recommencing education and research
Assessing the condition of damaged buildings and estates infrastructure
Facilitating building repairs and the reinstatement of utilities and equipment
Overseeing salvage operations and project management of estates recovery activities
Overseeing the recovery of contracted services (Catering etc.)

4.2.4 ITS Disaster Recovery Group– Led by the IT Disaster Recovery Coordinator

Key Tasks - Facilitating restoration and renewal of IT hardware, software and infrastructure.
Recovery of IT systems, data, telephony, website and connectivity and ensuring IT service continuity.
Providing UIMT with a timeline for the recovery of networks, key systems and applications.
Prioritising the restoration of IT systems and applications in line with the needs of the University.

4.2.5 Finance, Legal & Insurance Recovery Group – Led by the Director of Finance and the General Counsel

Key Tasks - Make emergency funds available whilst continuing to pay existing creditors
Accounting for incident expenditure and maintaining an inventory of losses
Liaising with regulators, insurers and loss adjustors.
Providing legal advice and ensuring that statutory reporting is completed on time.

4.3 Professional Services - Priority Activities

These following Professional Services will be given priority for resumption due to the potential University-wide impact of interruptions:

Service	Priority Activities	Possible mitigation if disruption occurs
IT Services	Providing operational data centres, IT systems, Network connectivity, telephony	Back-up data centre on Campus Off-site data centre
Estates (to include services provided by SEF)	Providing safe, secure and functional facilities and infrastructure across the entire University estate, Repairs and restoration	Security Team mobilised, Severe weather response, Identifying and sourcing alternative facilities and equipment (e.g. generators for emergency power)
Communications	Internal and External Messaging and Statements	Web information, email social media updates, App notifications
Finance & HR	FMS, Payroll, Insurance advice and welfare arrangements	Secure alternative locations, redeployment of staff

4.4 Partial or Phased Recovery

During a major incident, LIMTs and/or Recovery Groups will undertake an initial assessment of the disruption and devise an action plan to achieve the recovery of priority activities. Early consideration should be given to the availability of equipment and utilities to provide safe and secure accommodation, teaching and study spaces, laboratories and offices. This will include the provision of sufficient systems and resources to support critical processes as well as suitable heating, lighting, welfare and sanitation facilities for personnel.

During the phased resumption of services following a major incident receive resources and the duration of any necessary transition period. Alternative accommodation and/or equipment should be sought if recovery time objectives are unlikely to be met by using existing facilities.

4.5 Review & De-Brief Following a Disruptive Incident

Following a significant disruptive event, the Chief Operating Officer will write a report to review the University's response and to capture learning. Heads of Schools and Professional Service Directors will feed into this process by de-briefing their teams to evaluate the impact of such incidents, to review the effectiveness of their response and recovery efforts and to propose future mitigation measures to improve resilience.

4.6 Evacuations and Welfare of Personnel

Emergency evacuations may result in people becoming separated from their belongings and requiring temporary shelter or ongoing support. If it is not possible to return to a building within 30 minutes of evacuation, Security or Campus and Residential Support will identify suitable facilities for emergency shelter until access is permitted.

4.6.1 Emergency Shelter

The University's Security Team will determine the need to provide emergency shelter for displaced people following an evacuation. Depending on the location of the incident and the number of people involved, the following facilities will be considered; Library Café and Study Area, the Meeting House, Eat Central, North Field Bar and East Slope Hub.

5.0 Roles & Responsibilities

5.1 Estates, Facilities and Commercial Services– to include Sussex Estates and Facilities (SEF)

Sussex Estates and Facilities (SEF) are responsible for the maintenance operations at the University's Campus, including the availability of buildings, grounds, footpaths, roads, car parks and utilities infrastructure. The SEF Service Centre will perform the initial response to maintenance defects and have plans in place to escalate an incident should the need arise.

Security (also provided by SEF) provide the University's primary response to emergencies and other disruptive incidents and maintain documented procedures for doing so. Many emergencies (e.g. where there is a threat to life, assets or the environment) may also cause disruption to the University's priority activities and therefore the response and recovery frameworks held in this Business Continuity Plan will be aligned with the Emergency and Business Continuity Plans produced by SEF.

It is essential that the University and SEF work closely together throughout the business continuity management cycle to ensure that the services delivered under the contract are resilient and capable of initiating the required response and recovery in order to safeguard priority activities.

To this end, the Head of Service Delivery will liaise with the SEF Partnership Director (in consultation with the Senior Risk and Resilience Manager) to ensure that adequate Business Continuity plans are in place to protect campus operations during emergencies and other disruptive events. This will include ensuring that proactive and reactive work is undertaken and recorded to ensure that equipment (e.g. generators, flood barriers etc.) is available to maintain critical activities (e.g. experiments using unique materials) and respond to incidents in a timely way.

5.2 SEF Response and Recovery Roles

The SEF Partnership Director holds ultimate responsibility for the emergency response and security services on Campus. The Partnership Director will be a key member of the Estates and Facilities Recovery Group and will report to UIMT as required.

The SEF Head of Campus Facilities Management will liaise with the Response and Recovery Teams with regard to any disruption to University facilities and the estate. This will include evacuations, campus safety and security, repairs to buildings, grounds, utilities, transport infrastructure and the oversight of development projects (in conjunction with the Head of Projects).

The SEF Operations and Customer Services Manager will support the response and recovery efforts by providing transport, helpdesk, logistics and reprographics. The Head of Campus Facilities Management will provide input to the Incident Response and Recovery Teams on residences, cleaning, housekeeping, portering and laundry issues. The SEF Partnership Director must inform the University's Director of Estates and Facilities or the Head of Service Delivery (Facilities Management) should any disruption affect SEF's priority activities and/or contractual obligations.

5.3 University Incident Management Team Leader

This role will normally be undertaken by the Chief Operating Officer or the Provost. The main responsibilities will include:

- To act as the Gold Commander during major incidents and coordinate the University's strategic response and recovery efforts.
- To identify emerging risks and threats to the continuity of the University's priority activities and make decisions which serve to protect them.
- To ensure that resources are available to facilitate an effective response and recovery to an incident affecting the University.
- To agree the communications strategy throughout the duration of the incident.
- To liaise with external partners during the response and recovery process.
- To approve and agree mutual aid protocols with key partners.
- To write a report following a major incident to capture any learning.

5.4 Local Incident Management Team (LIMT) Leaders

Schools and Professional Services should prepare for and respond to local incidents by forming a Local Incident Management Team (LIMT) from within their ranks, to oversee the tactical management of incidents. The Head of School or Professional Services Director (or equivalent) will act as the LIMT Leader and will be responsible for:

- Scenario planning and assessing the risk of disruption to priority activities within their area of responsibility, known as an activity Business Impact Analysis (BIA).
- Identifying and resourcing suitable risk mitigation measures which maintain resilience.
- Ensuring that sufficient resources are allocated to business continuity planning to protect teaching, research, enterprise and key support services.
- Ensuring that all staff are aware of the arrangements for dealing with disruption and that there are sufficient competencies within the school/service to manage incidents.
- Acting as Silver Commander and overseeing the tactical response to local incidents within their School/PSD.
- Overseeing the activities of the Incident Response and Recovery Team Leaders within their School/PSD.
- Notifying the UIMT Leader if the incident requires strategic oversight and decisions.
- Notifying the relevant senior academics within the affected School(s)
- Working with the Risk and Resilience Senior Manager to develop a testing programme in order to validate local BC plans.

5.5 Incident Response & Recovery Team (IRRT) Leaders

The IRRT Leaders will be appointed by LIMT Leaders to prepare for incidents within Schools/PSDs and facilitate the local response and recovery. The main responsibilities will include:

- Maintaining documented Incident Response and Recovery Plans and ensuring that business continuity is included in the School/Divisional emergency procedures.
- Maintaining contact lists and call-out arrangements to ensure that team members understand their role during incident response and recovery and that their contact details are kept up-to-date.
- Undertaking a service specific BIAs, to assess the impact of disruptive incidents upon the School/Division.
- To report any concerns to the relevant Head of School/Professional Services Director and agree the necessary course of action in order to manage any risks and vulnerabilities.
- Being the first responder to local incidents (acting as Bronze Commander) to oversee the operational response to emergencies and disruptive incidents, and to initiate the School's/Division's pre-agreed alternative working arrangements, as necessary.
- Facilitating and attending emergency and BC planning activities, exercises and tests.

5.6 Director for IT

Member of UIMT and owner of resilience arrangements for the technology environment.

The main responsibilities will include:

- To identify, monitor and mitigate risks within the technology environment which may affect the University's strategic objectives.
- To maintain and develop the technology environment to ensure that resilience is central to the University's IT strategy.
- To oversee cyber security and oversee the programme of work that serves to mitigate the risk of disruptive cyber-attacks, which may result in the loss of data or denial of access to technology systems and applications.
- To develop and maintain suitable response and recovery plans for coping with cyber-related incidents.
- To ensure that the procedures within the ITS Disaster Recovery and Service Continuity Plans are fit-for-purpose.
- To Chair meetings of the IT Disaster Recovery Team.
- To report on the recovery of IT systems, data and connectivity during a major incident and agree the communications strategy.

5.7 The IT Disaster Recovery Coordinator

The IT DR Coordinator will be appointed by the Director for IT.

The main responsibilities will include:

- To oversee the IT BIA process and report technology risks to the Director of IT Services.
- To monitor key dependencies placed upon IT Services in relation to the activities of Schools and Professional Services and to prioritise the most critical functions when responding to incidents.
- To maintain, test and review the IT Disaster Recovery Plan.
- Evaluating the plans of external service providers and suppliers, identifying potential risks and implementing improvements to protect IT services.
- Supporting the delivery of Incident Management training activities in conjunction with SEF and the University.
- Maintaining the testing and exercising programme to validate the IT DR and Service Continuity Plans.
- Implementing lessons learned following BC/ITSCM exercises and incidents.
- Issuing the ITSCM status report to the Director of IT Services during an incident.
- Ensuring that an operational role is assigned, with the responsibility for providing the UIMT with information, analyses and potential solutions during a major incident.

5.8 The Director of Communications, Marketing and Advancement

Member of UIMT responsible for the approach to crisis communications.

The main responsibilities during a major incident will include:

- To ensure that the University communicates with all relevant stakeholders in a timely and effective way.
- To monitor media interest and oversee the publication of official statements in relation to the incident.
- To ensure that relevant staff are suitably trained, briefed and available to give media interviews.
- To maintain and adhere to the procedures held within the University's Crisis Communications Plan.
- To ensure the continuity of other critical events and activities within service areas e.g. Graduation, Clearing.

5.9 Director of Human Resources

Member of UIMT and owner of resilience arrangements for human aspects of emergencies and business continuity incidents, in relation to staff, volunteers, visitors and contractors.

The main responsibilities will include:

- To oversee the development of policies and procedures for alerting key staff, enabling remote working, reviewing travel and succession planning in order to improve organisational resilience.
- To maintain suitable contractual arrangements for the relevant staff to ensure that the University's out-of-hours incident response capability is suitable and sufficient.
- To support the delivery of incident training and awareness activities, to improve competence among staff.
- To identify, monitor and mitigate risks which can affect staffing levels and disrupt the University's priority activities, such as industrial action and pandemic illness.
- To liaise with the relevant Trade Unions prior to and during industrial action and other disruptive incidents.
- To lead on staff welfare during the response to and recovery from an emergency or other disruptive event.
- To ensure the resilience of the staff payroll function, to include alternative office(s) and remote working etc.
- To ensure the continuity of other critical activities within relevant service areas.

5.10 Director for the Student Experience

Member of UIMT and owner of resilience arrangements for human aspects of business continuity – students, their families and friends

The main responsibilities will include:

- To lead on the student services response and prioritise student wellbeing during a major incident.
- To co-ordinate the response of Student Wellbeing & Residential Services, Study Abroad etc. (including out-of-hours) in consultation with colleagues from CMA, SEF (Security) and Estates.
- To identify students who may be particularly vulnerable during an incident and prioritise support accordingly.
- To assume ownership of specific people (student) risk mitigation plans.
- To liaise with the University Health Centre and public health authorities in managing the risk of pandemic illness within the student community.
- To provide chaplaincy and counselling services to support those affected by an incident, including friends and family members.
- Providing support and information for the management of student alerting and notification systems.
- To monitor risk and maintain plans for responding to incidents that may affect students who are overseas.
- To ensure that critical student facing services have plans for responding to disruptive incidents.
- To ensure the continuity of any other critical activities within relevant service areas.

5.11 General Counsel and Director for Governance and Compliance

The main responsibilities will include:

- To oversee the maintenance of the University's Business Continuity Policy and this Plan.
- To provide legal advice to the Crisis Management Team (CMT) and University Incident Management Team (UIMT) so as to ensure compliance with relevant legislation during the response to a disruptive incident and to support the recovery process.
- To provide advice to UIMT on matters relating to risk, business continuity and resilience when preparing for and responding to incidents.

5.12 Senior Risk & Resilience Manager (Adviser to UIMT)

The main responsibilities will include:

- To raise awareness about resilience and promote good practice across the University.
- To raise awareness of the University's Business Continuity arrangements.
- To provide advice and support to managers during disruptive incidents.
- To review the relevant University Plans and risk registers following an incident.
- To liaise with Local Resilience Forum partners as necessary.

5.13 Procurement Manager (Adviser to UIMT)

The main responsibilities will include:

- To ensure that procurement policy and procedures give due consideration to business continuity risks and seek sufficient assurance from suppliers and contractors during the tendering process.
- To advise on the procurement process during the recovery from a disruptive incident.

5.14 Insurance Manager (Adviser to UIMT)

The main responsibilities will include:

- To liaise with the University's insurers and provide advice in order to treat business continuity risks.
- To ensure that the University's insurance cover for foreseeable incidents is suitable and sufficient.
- To advise on the cover available for University personnel who have been affected by an incident.
- To work with the University's insurers to support the timely and effective allocation of emergency resources throughout the recovery process.
- To work with loss adjustors following a disruptive incident and advise on the implementation of salvage and recovery processes.

5.15 Associate Director of Communications (Adviser to UIMT)

The main responsibilities will include:

- To maintain the University's Crisis Communications Plan.
- To oversee internal and external communications during an incident and to ensure that the University's methods of communicating are resilient.
- To ensure that crisis communication resources are available and tested routinely, to provide assurance of capability during incidents and exercises.
- To maintain a capability to monitor and respond to media and social media coverage about an ongoing incident in a timely way.

5.16 Heads of Schools, School Coordinators, Senior Academics and other Professional Services Directors (Co-opted Advisers to UIMT as necessary)

The main responsibilities will include:

- To support response and recovery activities by maintaining and implementing specific local incident response and business continuity plans.
- To assist in the strategic response by informing and advising UIMT of the local impact and any ongoing risks, as necessary.
- To assist in the tactical management of the incident by working in the Business Recovery Teams as specified in Section 4 of this document.

6.0 Business Continuity Guidance - See Section 1.0 for further information

6.1 What is Business Continuity Management?

Business Continuity Management is a cyclical process which helps us to prepare for and respond to disruptive events. A Business Continuity Plan is a written record of pre-agreed procedures for responding to incidents, with guidance for key staff.

6.2 Why is BCM important?

Business Continuity planning will make the University more resilient and potentially reduce the risk of disruption. The objective is to assess the risks to 'business as usual' operation, identify and give priority to the most critical activities and develop pre-agreed arrangements for alternative working to acceptable levels should disruption occur. Resilient teams do not become a burden to others when dealing with disruption, they find and manage their own solutions.

6.3 How can I prepare for disruption?

Identifying that your School or Division may be vulnerable to disruption is the first step. This is known as Business Impact Analysis (BIA). All staff should be vigilant and inform management of any activities that may be particularly vulnerable to certain types of disruption. Plan your activities assuming that access to facilities and the availability of IT or utilities may occasionally be interrupted. Consider your ability to make quick decisions and establish alternative ways of working should this be the case. It is a good idea to identify requirements and agree alternative arrangements in advance.

The next stage is to undertake a risk assessment to identify realistic scenarios which could lead to the loss of workspace, personnel, IT, utilities, unique materials, critical equipment and supplies.

The extent of disruption can vary widely from relatively short-lived events affecting only a few activities, such a utility outage to more widespread incidents, long-lived incidents, such as a pandemic. In addition to the impact, it is important to examine the likelihood of disruption occurring before mitigation measures can be properly considered. In practice, short-lived, lower impact events may occur more regularly and therefore procedures for responding to these may feature more prominently in your BCP. Such incidents may simply require the adoption of alternative working arrangements for a short while, but it is still advisable to plan these measures in advance. Once the threats are known, you can begin to plan contingency measures in order to control the risk of disruption and identify the resources required for recovery. Suggested mitigation measures to be included in a Business Continuity Plan:

- Alternative space or remote working (for teaching, research, study, office work, storage etc.)
- Emergency communications protocols - contacts lists, incident log, procedures
- Emergency equipment – generators, back-up memory sticks, radios, torches
- Secondary (off-site) storage for essential/unique materials, equipment, records and data.

6.4 How do I know the plan will work?

Discuss BC with your team so that they are prepared to respond to incidents. Test your plans using realistic scenarios (e.g. outages, flood, fire, flu etc.). Manage expectations, remember that your 'Plan B' does not have to involve working at full capacity, just to a pre-defined, acceptable level. Review your plan based on any lessons that you learn from incidents or exercises. The Senior Risk and Resilience Manager will provide support if required.

Part 2 – (a) Business Continuity Plan Template

School/Service:
Normal Campus Location(s):
Facility requirements and key BC dependencies: *e.g. 2 labs requiring uninterrupted power, office with 12 desks/pcs*

	Location		
Record of Critical Equipment, Unique Materials and Assets of High value/importance	**Building**	**Floor**	**Room Number**

Local Incident Management Team Contact Details:

Name:	**Job Title:** *(NB - include the following)*	**Mobile Number:**
	Site Incident Manager - Bronze	(include Out of Hours)
	Head of School/Director - Silver	
	Team Leader(s)	
	Administrator(s)	
	Technical Services Manager	
	SEF Building Manager	
	Estates/IT/HR/Comms Lead	

Preparedness - Procedures for Continuation of Priority Activities:

This plan is to be invoked by the Head of School/Director (or his/her deputy) should a disruptive incident occur which means that time-critical, high priority activities are interrupted.

The Head of School/Director (or his/her deputy) is responsible for undertaking an initial assessment of the damage and/or disruption. Should evacuation be necessary, a member of the team should be prepared to collect the 'Grab Bag' for your building (if applicable) and staff will adopt pre-agreed alternative working arrangements.

The Head of School/Director (or his/her deputy) is responsible for informing the team of the disruption and implementing alternative working arrangements to enable the continuity of the priority activities whilst ensuring the safety and well-being of staff.

The Head of School/Director (or his/her deputy) is responsible for informing UIMT of the disruption to normal business and the invocation of the local BC plan.

Action Plan:

Use the table below to describe how certain routine functions may be suspended to protect the most critical activities when disruption occurs:

Priority activities to be continued:	**Staff required:**	**Facilities/Equipment required:**
e.g. critical research, statutory reporting		
Activities that may be suspended:	**Staff diverted:**	**Resources made available:**
e.g. back office admin		
Target Time for Recovery of Priority Activities:		

Agreed Alternative Working Arrangements:

e.g. remote-working, pre-agreed secondary office location, staff re-deployment, reduced operating capacity, 'pen and paper' working, emergency power supply to sustain critical activities.

Are unique materials/essential equipment/data protected and accessible elsewhere? Y/N

Details of Emergency Equipment & Supplies:

A reserve supply of the most vital materials equipment you need to perform priority activities

Emergency equipment or materials:	**Location:**
e.g. Red Box/Grab Bag/Stationery	

Suggested 'Grab Bag' contents: Duplicates of any specialist equipment, secure copies of important files, hard copy of this plan, incident log, stationery, PPE, torch, radios, loudhailer etc.

Preparedness - BC Plan Development and Review:

This Plan has been developed so that the School/Division will be able to respond to a disruptive incident, whilst ensuring that working conditions are safe and secure.

The School/Division's activities have been risk assessed and the most urgent tasks have been given priority for resumption.

All staff are aware of the procedures in this plan and have been involved in their development. Staff have been made aware of their responsibility towards securing office equipment, including sensitive materials and data.

The procedures held in this Plan will complement those in the University's Business Continuity Plan and will be invoked accordingly.

This Plan will be validated with an exercise in consultation with the Risk and Resilience Manager.

This Plan will be owned by the Head of School/Director and reviewed annually, or following an applicable incident, in consultation with the Risk and Resilience Manager.

Calendar of Critical Activities (*particular events when recovery times become more urgent***)**

Date/Month	Activity	Recovery time	Specific BC Plan?

Record of Amendments to this Plan

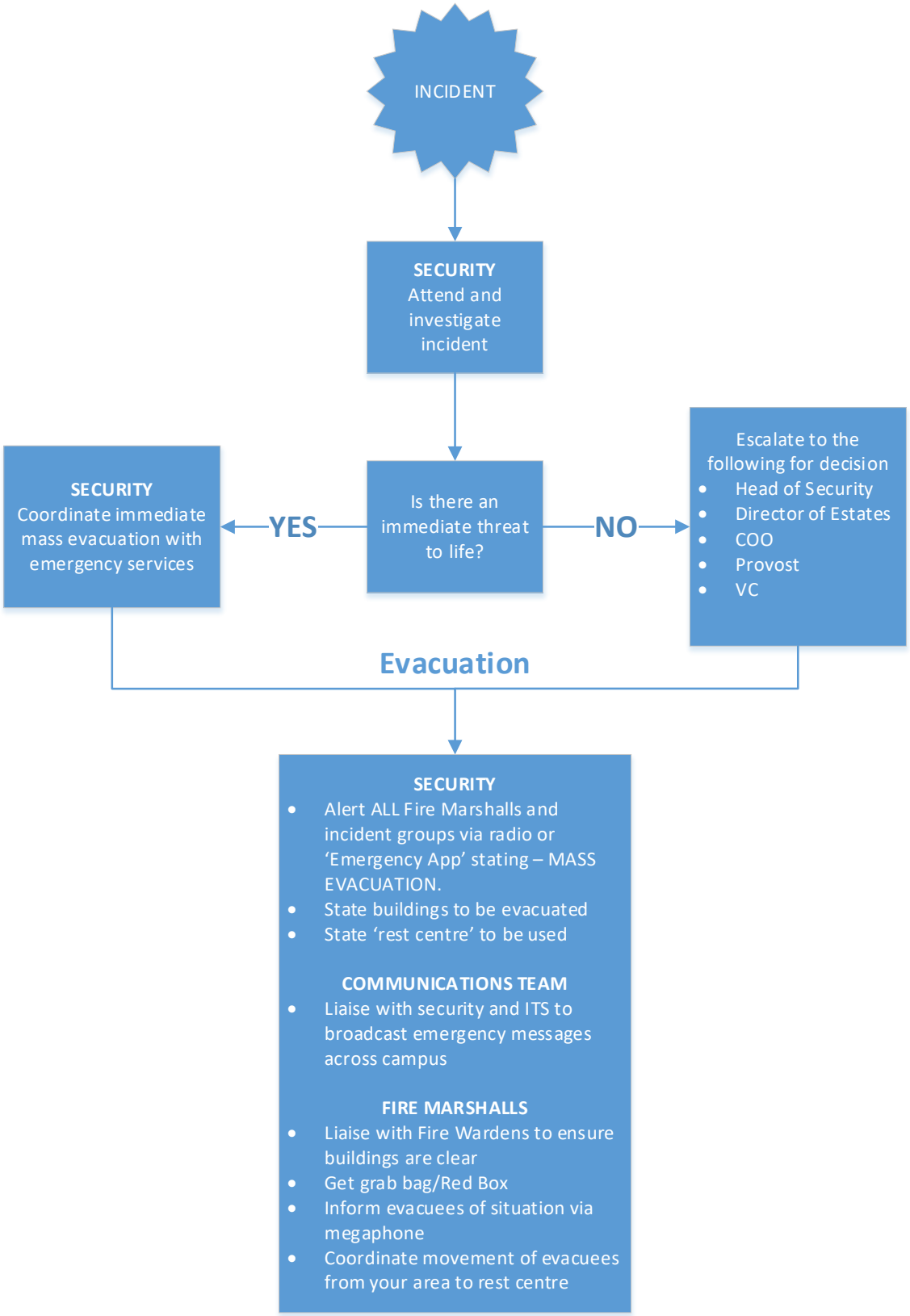
No.	Amended section (s)	Date
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Incident Response – Checklist for Site Incident Manager

No.	Actions	✓
1	Evacuate as instructed, liaise with Fire Warden or assume the role if no-one else presents	
2	Ensure you have a tabard, ID card, 'Grab Bag' and 'Red Box' (if applicable)	
3	Receive report of incident from Security/Emergency Responders	
4	Assess initial impact of damage/disruption – prepare Situation Report (SITREP)	
5	Invoke BC Plan, start an incident log (p.8) and continue to update	
6	Remain at incident scene if safe to do so, attend if requested (if offsite)	
7	Senior responsible person on scene to act as Site Incident Manager (Bronze)	
8	Assess the situation (Scale, Duration and Impact) and liaise with other University responders	
9	Liaise with emergency services Incident Commander(s) (if in attendence) and take contact details.	
10	Consider shelter options if evacuating staff and students (See evacuation flowchart)	
11	Inform the following as necessary; - Local Incident Management Team (see contacts list P.1) - Building Manager(s) - Cleaning/Maintenance Staff - Residential Support Managers (if applicable)	
12	Escalate to the following as necessary; - Head of Security - Head of Campus and Residential Services	
13	Liaise with security office to ensure School/Divisional emergency contacts are aware of any incident that affects them.	
14	If press or media are in attendence, inform them that CMA colleagues will brief them ASAP. Inform Security Control room of media interest	

NB – for further information you should also refer to the University's Incident Response Guidance document.

Incident Response - Evacuation Flowchart:



Incident Response – Action Card

Detect and describe incident

- Initial notification - alert emergency responders, start the incident log, take Grab Bag
- Arrival at the scene, maintain safe distance and gather initial information about the incident
- Senior responsible person becomes Site Incident Manager (Bronze Commander)
- Update emergency responders using METHANE report - Is this a Major Incident?
- Notify senior (Silver/Gold) commanders and escalate if additional support is required
- Provide SITREP - describe what is happening, where and who/what has been affected

Protect life and property

- Prioritise safety at the scene and control access
- Dynamic risk assessment - monitor hazards and maintain safe distance
- Assess casualties and provide first aid as required
- Speak to witnesses - is anyone else believed to be injured, trapped or missing?
- Evacuate affected areas as necessary
- Formalise safety cordon and incident control point with emergency responders, as necessary
- Liaise with emergency services to safeguard critical assets and update senior commanders

Support those afftected

- Communicate with those directly affected at the scene (e.g. displaced people)
- Be prepared to evacuate a wider area, if advised to do so by emergency services
- Arrange temporary shelter for displaced people - a place of warmth with catering, toilets etc.
- Support people who have lost access to personal belongings or critical research materials
- Alert the Communications Team to warn and inform community and respond to enquiries

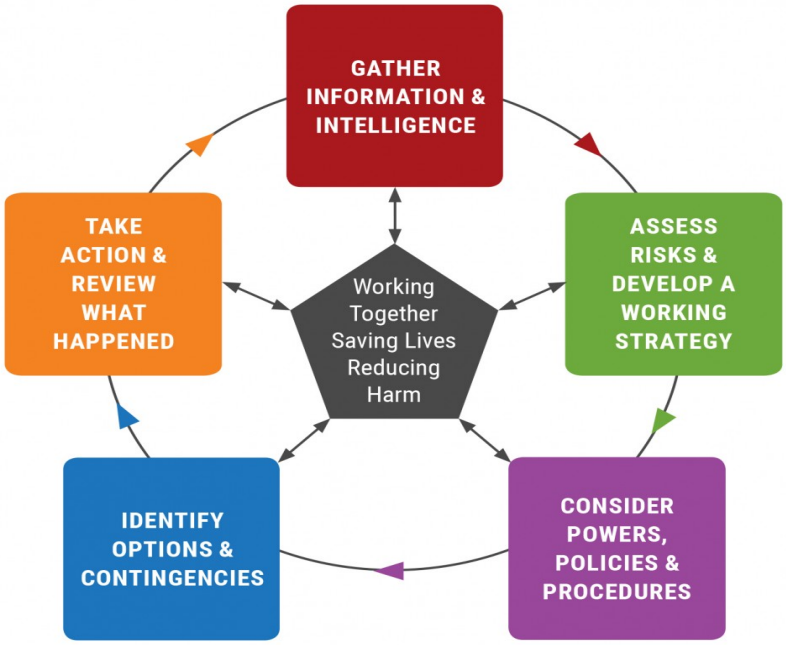
Mitigate impact of incident

- Invoke Emergency/BC Plans and call out designated staff (e.g. specialist advisers as on P.1)
- Continue to maintain incident log of all noteworthy events and actions taken with timelines
- Provide updated SITREPs to Silver/Gold on a regular basis
- Brief Silver/Gold Command to confirm decisions and actions
- Inform Communications Team to manage messaging
- Ongoing evaluation of impact and resource requirements
- Set recovery strategy

Plan for recovery

- Commence initial assessment of losses, salvage activities and ongoing risks
- Continue to inform staff, students and stakeholders about the impact and action taken
- Arrange de-brief to capture lessons learned
- Evaluate risk of future incidents
- Review incident response arrangements - resources
- Review business continuity and recovery plans - documentation

Incident Response - Decision Making Aide Memoire



Incident Response Guidance – General Principles

Gather and Share Information

- What has happened and how are we responding? Is this a Major Incident?
- Site Incident Manager to report the scale of the incident (SITREP). Open Incident Log.
- Is Escalation necessary? Who should be informed as a priority at this stage?
- Alert the Communications Team to inform the community and monitor media coverage.

Risk Assessment

- Preserve life - safety and welfare check to identify any immediate hazards or threats.
- Assess the initial impact of the incident and how the effects can be mitigated.

Establish Command and Control

- Determine the need for escalation, technical expertise and leadership – e.g. Silver/Gold command.
- Notify key personnel as necessary, including out-of-hours notification.
- Liaise with emergency responders and agree location of Incident Control Point, as necessary.

Objective Setting

- Prioritise the safety of personnel and identify any urgent issues for immediate action.
- Evaluate response capabilities and secure additional resources to support recovery.
- Liaise with insurers and engage with stakeholders.

Establish Communications Strategy

- Quickly acknowledge what has happened and inform the University community.
- Provide details of the ongoing response and recovery efforts.
- Manage the initial surge of enquiries and the flow of information.
- Monitor media coverage and provide regular updates to all stakeholders.

Incident Response - Business Continuity Incident Log

School/Service/Team:	**Person completing this Log:**
Nature of Incident:	**Time/Date:**
Are all personnel accounted for? Y/N	**Casualties? Y/N**
Emergency services required? Y/N	**Emergency services contacted? Y/N/NA**
Is any critical equipment/unique material/valuable asset compromised?	**Location(s) affected:**
BC Plan invoked? Y/N	**Emergency Plan activated? Y/N**

SITREP – An initial assessment of damage/disruption:

Hazards/Threats:	**Access:**

Communication – Have the following been informed?

Staff (who are not present)	**Y/N/NA**
Students	**Y/N/NA**
SEF	**Y/N/NA**
ITS	**Y/N/NA**
Contractors	**Y/N/NA**
Communications Team	**Y/N/NA**
HR	**Y/N/NA**
UIMT	**Y/N/NA**

Log of Decisions and Actions:	
Time:	**Details of Decision/Action and Rationale:**

UNIVERSITY OF SUSSEX

Part 2 – (b) Business Impact Analysis Template

Priority Activity:	
Key Dependencies:	*People/Facilities/Utilities/IT/Supplies/Equipment*

Effect of Disruption on Service/Activity:

Time	Effect of Disruption on Service:
First 24 hours	• • •
24 – 48 hours	• • •
Up to 1 week	• • •
Up to 2 weeks	• • •

Resource Requirements for Recovery:

Time	No. of staff	Relocation?	Resources required	Data required
First 24 hours			• • • •	• • • •
24 – 48 hours			• • • •	• • • •
Up to 1 week			• • • •	• • • •

Appendix 1 – Suggested Agenda for UIMT Meetings

UNIVERSITY OF SUSSEX

University Incident Management Team

AGENDA

1. Introduction, Apologies and Wellbeing Check

2. Brief Description of Incident

    - SITREP from IRRTs/LIMTs - What do we know? What must we assume?
    - Major Incident Declared? Y/N

3. Set Strategic Aim

4. Urgent Priorities for Immediate Action

    - Initial statement to be agreed and issued

5. Note the Key Risks, Proposed Mitigation Measures and Agree Ownership

6. Additional Resources Required for Recovery

7. Finance & Insurance

8. Communications Strategy

9. AOB

10. Date/Time of Next Meeting

Appendix 2 – UIMT – Major Incident - Initial Action Checklist

Action Required	By Whom	By When
Convene meeting of UIMT in an appropriate location or remote		
Appoint Secretary (Loggist) to note decisions and actions		
SITREP - Receive initial incident report detailing any damage/disruption		
Note the impact to the University's activities/personnel – prioritise safety and welfare		
Urgent communications – agree initial statement		
Initiate welfare checks and confirm ongoing support for personnel		
Plan ahead - What do we know? What must we assume?		
Agree primary recovery objectives and resource requirements		
Prepare briefings for ULT, Chair of Council etc.		
Confirm insurance cover and arrangements for emergency expenditure		
Record disrupted activities and note details of any alternative provision		
Consider making a 'mutual aid' request to local partners		
Liaise with Local Resilience Forum partners		
Form Business Recovery Groups and commence recovery workstreams		

Appendix 3 – Business Recovery Groups (BRGs) - Initial Action Checklist

Action Required	Which BRT?	By When
Convene meeting of BRGs as directed by UIMT – in person/remote	All	
Evaluate the damage, disruption, environmental impact and any ongoing risks/threats	All	
Plan to recover - What do we know? What must we assume?	All	
Identify primary recovery objectives and resource requirements	All	
Uphold duty of care towards personnel, warn and inform	BRG – Estates/Personnel	
Initiate welfare checks and provide ongoing support for personnel	BRG - Personnel	
If evacuation has been necessary, identify and provide temporary shelter and/or emergency accommodation	BRG - Estates	
Liaise with emergency responders to protect the scene	BRG – Estates	
Commence recovery of key systems, services and infrastructure	BRG – Estates/IT	
Commence salvage and reinstatement activities	BRG – Estates/IT	
Investigate alternative facilities/space to deliver priority activities	BRG - Estates	
Inform and liaise with insurers and loss adjusters	BRG – Finance/Legal	
Provide legal advice and emergency expenses	BRG – Finance/Legal	
Inform Incident Managers and CMA of decisions	All	
Report emerging risks and agree frequency of future meetings	All	