University of Salford MANCHESTER

Emergency Planning Policy

Version Number 3.0

Effective from December 2021

Authors: Head of Security, Estates and Facilities

Document Control Information

Revision History incl. Authorisation: (most recent first)

Author	Summary of changes	Version	Authorised & Date
T Jones	Minor revisions and updates reflecting managerial changes	V.3	Ass Dir Estates December 2021
T Jones	*Minor revision and updates reflecting management changes.* *Amended GDPR Reference*	V2.2.A V2.2	Executive Director Estates and facilities 10/10/18
C. Price & T. Jones	*Minor revisions and updates reflecting organisational restructures*	V2.1	Executive Director Estates, Facilities & IT Services: 01/04/2016
C. Price & T. Jones	*Revision to incorporate business continuity requirements for University*	V2.0	Ops Board: 17/12/2014
C. Price & T.Jones	*New Incident management policy*	V1.0	Exec: 23/04/2012

Policy Management and Responsibilities:

Owner:	This Policy is issued by the COO, who has the responsibility for Emergency Planning on behalf of the University. The Director of Estates and Facilities Services has the authority to issue and communicate policy on Emergency Planning (including Business Continuity) and has delegated day to day management and communication of the policy to the Head of Security, EF.
Others with responsibilities (please specify):	All subjects of the Policy i.e. University and its 3rd party occupiers will be responsible for engaging with and adhering to this policy.

Author to complete formal assessment with the below advisory teams:

Equality Analysis (E&D, HR) *Equality Initial assessment form*	1. *March 2016, Low risk, saved to V drive with word version of policy.*
Legal implications (LPG)	2. *N/A*
Information Governance (LPG)	3. *March 2016 as part of policy template update*
Student facing procedures (QEO)	4. *N/A*
UK Visa & Immigration team (Student Admin)	5. *N/A*

Consultation:

Staff Trades Unions via HR Students via USSU Relevant external bodies (specify)	1. N/A 2. N/A

Review:

Review due:	2 years by November 2023
Document location:	University Policy & Procedure Pages (Estates section)

http://www.salford.ac.uk/about-us/corporate-information/governance/policies-and-procedures

Document disséminations and communications plan:
US Online article, In Brief strategic update, MIT training content

1.0 Purpose

The purpose of this document is to specify the University Policy on both Major Incident Response and Business Continuity Management, collectively known as 'Emergency Planning'. The University is committed to maintaining Business Continuity, encouraging the resilience of the organisation through development and documentation of Business Continuity Plans by all Schools and Professional Services and to support continuance or rapid recovery of critical operations. The University is also committed to protecting the interests of students, staff and all relevant stakeholders in the event of an emergency or business disruption by using Emergency Planning and supporting response models.

This Emergency Planning Policy and supporting work is underpinned by the following principles, to ensure that:

- students and staff members receive clear communications and direction in the event of any disruption;
- the Major Incident Team members have undergone mandatory Emergency Planning training, have good and timely decision making skills and can adapt according to the situation (i.e. not too rigid a view of only 1 possible solution);
- the University is prepared and capable of protecting its reputation, core activities and brand in the event of disruption;
- the University remains compliant with its legal and regulatory obligations.

This policy is based on and incorporates elements of International Standard BS ISO 22301:2012 and 22313:2012 and the AUCSO Resilience in Higher Education Guide (2014).

2.0 Scope

2.1 To whom the policy applies

This policy applies to all members of the University including (but not limited) to: students, staff, contractors, visitors, University tenants / 3rd party occupiers and partner organisations including the Emergency Services. Particular attention should be taken by members and potential members (as may be called upon) of the University Major Incident Team.

2.2 Aims of the policy

This policy outlines:

- key arrangements for responding to Major Incidents (Major Incident Plan - MIP)
- high level structure and responsibilities of the 3 levels in a Major Incident Team (MIT) i.e. gold, silver and bronze
- management support and direction for Business Continuity (BC)
- requirement for Schools and Professional Services to develop and submit Business Continuity Plans covering priority services, resources, contacts and recovery arrangements. Yearly updates to all plans are required
- relationship between Major Incidents and Business Continuity, particularly the circumstances in which the Business Continuity plans may be invoked

2.3 Definitions

Emergency Planning: overarching term which the University will use to refer to Incident Management and Business Continuity i.e. any disruptive incident that is out of the ordinary.

Major Incident: actual or anticipated event which threatens serious damage to:

a. Welfare of students or staff
b. Ability to provide teaching, learning and research activities
c. Ability of the University to conduct its normal activities
d. The University's reputation
e. The University's property
f. The University's information, **and**

is beyond the scope of resolution by normal decision-making mechanisms.

Major Incident Team (MIT): Consists of relevant staff at one of three levels of incident response;

Strategic (Gold)	Tactical (Silver)	Operational (Bronze)
Gold Command	Silver Command	Bronze Command
COO or alternative Senior Manager that is suitably trained and deemed competent. Decision-making for situations with far reaching consequences (over and above Silver command) Supported by Loggist	Major Incident Team led by a suitably trained and competent Team Leader Directs the response Often Heads of Service and Heads of relevant Schools carrying out core decision making functions Supported by Loggist	Incident Responders On-site hands-on work to implement the response - either fixing the problem, - or mitigating the impacts e.g. on students
Board room level	Use 'Incident Management Suite' in the Maxwell Hub	'At the scene' 'In the area where mitigating actions are needed'

Note: As Chief Executive Officer of the University, the Vice Chancellor sits outside the MIT structure but is consulted on key decisions and will deal with Council and external matters as appropriate.

Major Incident Plan (MIP): The plan which the Major Incident Team will use to manage the University's response to a major incident. The MIP includes standard emergency responses such as building evacuation or dealing with hazardous substance release and a number of linked documents, checklists, standard escalation routes and individual actions for managing the incident. The MIP is managed by the Head of Security, Estates, Facilities & IT Services.

Duty Manager: These are four operational managers from Estates, Facilities & IT Services; of whom one will be available 24 hours a day on a weekly rota to deal with and respond to any

incident affecting the safety and security of daily business. The Duty Manager will be responsible for contacting the VC (or delegate in charge of the University at that time) to gain relevant authority to invoke a Major Incident and initiate the tactical (silver) Major Incident Team. The VC (or delegate) will appoint a Gold Commander for the incident.

Loggist / Record Keeper: The Loggist's role is to support the Chair at Gold and Silver command by recording all decisions and agreed actions. It is important that factual information is recorded as the records may have to be produced at a public inquiry or court of law.

Business Continuity Management: re-instatement of University services and provisions. This recovery process may continue to run parallel to an incident after the initial response.

2.4 What the policy does not cover

This policy does not specify:

1. All role holders within Major Incident Team (this will vary according to the incident and a published list of contacts can quickly become out of date)
2. Exact detail of response plans or business continuity plans. These will vary according to the priority services and activities as identified by each owner i.e. Head of School or Professional Service.

3.0 Policy Statements

3.1 Management Commitment

The COO is responsible for emergency planning (and by association business continuity) on behalf of the University. Day to day management of emergency planning is the responsibility of the Director of Estates, Facilities and IT Services. The COO and Director of Estates require the support of all Heads of School and Professional Services to build resilience into the University's services and to be better positioned to survive and continue business in the event of a major disruption.

3.2 Responsibilities

Silver Command leader will: on approval from the Gold Command invoke a Major Incident response and convene the MIT. The MIT (Silver team) will assemble to deal with the immediate response and to prioritise the major incident recovery activities across the affected areas. Regular reports and strategic decisions will be referred to Gold Command as and when necessary. The MIT will be supported by trained Loggists to record all decisions and agreed actions. Large-scale incidents and those shown to have a criminal intent may be led by external agencies such as Police, Fire or Health & Safety Executive.

Estates & Facilities staff is responsible for premises, security and first-aid incidents, often via the Security team and / or Duty Managers. In the event of a major incident, the Division will also be involved in identifying suitable interim office and teaching spaces on behalf of the University. This is dependent on clearly identified and communicated requirements in School's and Professional Service's BC Plans.

IT Services staff is responsible for provision of network services and centrally managed data centres. In the event of a failure of one or more IT services (or hardware platforms) that causes significant disruption to business operation which cannot be recovered within the agreed recovery time for the service, IT Services will invoke the IT Systems Disaster Recovery Procedure. In the event of a major incident, IT services will be involved in the MIT and respond to IT requirements as requested by Estates (as identified in the BC Plans).

Each **Business Owner** (i.e. Heads of Professional Service and Heads of School), is considered to be the expert in their area and is responsible for maintaining an up to date Business Continuity (BC) Plan which will be reviewed annually as part of the Operational Planning cycle. The BC Plan identifies:

a) Core activities, their priority and dependency on other teams or actions
b) Core resources (equipment, furniture, space etc) required to carry out those activities, with an emphasis on the bespoke resources that their area needs (that are not commonly used / easily replaced)
c) Key suppliers and contacts that may be needed in the event of an emergency
d) Agreed recovery arrangements that the BC Plan Owner may be directed to invoke in the event of a major disruption.

The Business Owner (BC Plan Owner) is also responsible for:

1. communicating the BC plan to staff within their area
2. ensuring those relevant staff have an accessible and up to date copy of the BC Plan

3. ensuring those relevant staff understand their role in the event of having to invoke the BC Plan
4. ensuring the Head of Security / Emergency Planning Co-ordinator holds a copy of the most recent BC Plan.

Partner organisations / University tenants: Estates and Facilities & IT Services will include BC and MIT requirements in occupation licences with each of our third party occupiers. The Building Managers will ensure that there is regular liaison with these occupiers to keep the occupiers emergency contact details in a register held by the Head of Facilities.

3.3 Resilience and Business Continuity Plans

Business Continuity Plans (BC Plans) complement the University Emergency Planning to ensure the University can not only deal with the immediate consequences of a Major Incident, but also consider the long term impacts on the University and where practical, improve its resilience. The University's business continuity approach is guided by the following core aims:

- Protect people from harm
- Protect critical infrastructure and facilities
- Resume teaching, research and key services in an appropriate timeframe, with the minimum of disruption
- Focus on mitigating the impact of disruption, not just on identifying the cause

The level of detail within BC plans will increase as Business Continuity planning matures, for example:

Years 2016/17: Continue to identify key activities together with supporting services, processes and resources and communicate the BC Plan to relevant staff.

Introduce a Memorandum of Understanding with relevant Universities. Additionally an Information Sharing Agreement should be in place to ensure compliance with the General Data Protection Regulation.

Years 2018/19: Additional assessment of Business Impacts. Implement a risk assessed approach to identify the types of disruptive incidents (most likely to affect University core services) and where possible take steps to reduce or prevent likelihood of those incidents. This should continue indefinitely

Year 2022L: Additional loggist training with loggist beginning to be on a Rota system. Gold Command will commence a new week on Gold Rota

3.4 Training

Completion of Training will be considered to be a mandatory requirement for relevant and nominated staff. The training will include a series of competency assessments and individuals will be required to attain a satisfactory standard of completion. Any member of staff failing to achieve the required standard will not be permitted to take part in a live major incident. There will be two training programmes available:

- Emergency Planning for MIT members (at the different incident response levels)
- Loggist training (to support record keeping during a Major incident).

These training events will be scheduled at least annually to ensure appropriate members of staff are able to demonstrate that they are trained and capable. This will also ensure compliance with audit and insurance requirements.

Equally, staff competency in dealing with real incidents will be reviewed and could result in staff members not being permitted to take part in future incident response.

3.5 Regular review and testing

BC Plans need to be regularly reviewed, updated and re-issued to relevant staff within the School or Professional Services area. Validation of Major Incident and BC Plans is essential; whether by walkthroughs, desktop scenario or active exercise in a time pressured live environment. The University will have a method of restoring key functions and services to the agreed levels within the agreed timescale and this will be rehearsed on an annual basis. Relevant staff members as identified in each BC Plan will need to be trained to know how to use them and most importantly where to find the Plans.

The requirement for regular review will be captured in the yearly operational planning cycle. However, where major changes occur or events that impact the Universities ability to carry out its core activities (e.g. staff restructures or widespread staff industrial action) the BC Plans should be revised prior to the operational planning cycle.

4.0 Policy Enforcement

Failure to adequately document and have available accurate Business Continuity Plans might have a considerable impact on the University in the event of a disruptive incident. Errors due to lack of planning or preparedness during a major incident, could lead to serious financial, legal and reputational damage to the University, from which it may not recover.

5.0 Related Documentation

The below documents are closely related to this Emergency Planning Policy. However these documents are confidential in nature and will not be published.

- IT Services Disaster Recovery Plan
- Major Incident Plans
- Business Continuity Plans
- Security Assignment Instructions

6.0 Appendices

Appendix 1: Major Incident Plan overview

Appendix 2: Major Incident Team Responsibilities

Appendix 1: Major Incident Plan Overview

- Linked documents, each with a complementary purpose:
  - Develop response
  - Implement response
- There is no need to wade through a tome to understand what needs to be done
- The role-based system operates more effectively using the workbook templates.

Major Incident Plan – Silver Team

- A ‘standard’ escalation route
- Colour coded sections give the documents a simple, visible structure
- Initial assessment
- Workbook provides an audit trail
- Allows the team to concentrate on the incident and not the process
- Initial agenda offers guidance when it is needed most
- Debrief process for post incident review.

Major Incident Plan – Silver Team Individual action plans

- Individual action plans allow MIT members to ‘kick start’ each role
- Optional tools are provided for support

MIT actions and decisions will be recorded by a Loggist to:

- Allow the MIT to accurately review progress during the incident.
- Provide evidence for:
  - Investigations
  - Insurance
  - Auditors
  - Assist with handovers
- Inform debrief activities

Major Incident Plan – initial escalation

Major incident – on-going response

After the initial response to the major incident the MIT will direct:

Infrastructure Recovery: where infrastructure services provided by Estates, Facilities & IT Services will recover first.

Business Continuity: where Schools and Professional Services relocate staff and work areas as required, in particular priority services and activities.

The above **recovery stages** may continue to run parallel to on-going management of a major incident.

Reinstatement: where all processes and activities are reinstated after recovery from the major incident. This may involve moving back to facilities occupied before the major incident.

Appendix 2: Major Incident Team Responsibilities

Gold (Strategic) Command

- Initiate the response.
- Be the ultimate decision makers.
- Keep a high-level view.
- Analyse long term impacts particularly affecting reputation.
- Keep the University Council informed.
- Consider the shape of the University's future service offering.

Silver (Tactical) Command

- Collaborate with all areas of the University.
- Ensure Business Continuity Plans are accessed, distributed and used.
- Manage, but do not get directly involved in, operational issues.
- Provide options for agreement by Gold Team, relaying decisions to Bronze.
- Deploy Bronze.
- Agree when to stand down and return to business as usual.

Seven core roles within Silver command with support from secretariat / decision loggist but may be changed dependant on scenario

1. Leader
2. Human Resources Co-ordinator
3. Communications Co-ordinator
4. Planning Co-ordinator
5. Estates & Infrastructure Co-ordinator
6. Professional Services Co-ordinator
7. Academic Co-ordinator
8. Loggist

Bronze (Core) Command

- Human Resources
- Communications
- Student Administration Directorate
- Estates & Facilities
- IT Services
- Finance

Non-core Bronze Command

- Heads of affected Schools and Professional Services
- The Library
- Residences
- Student's Union