



Version	1
Author	University Secretary
Approving Body	UEB, endorsed by Audit Committee
Approval Date	10 th August 2022
Review Date	3 years after approval
Accessibility Checked	12 th May 2022
Equality Impact Assessment	N/A

1.1 The University of Worcester is committed to the development and implementation of business continuity, appropriate to the scale, nature, complexity and geography of the University, and the relevant environments in which it operates. We believe that the way in which we plan, prepare, respond to, and learn from, incidents is key to our overall effective recovery. Business Continuity Management plays a critical part in the University's overall control environment.

1.2

Business Continuity Management (BCM) is concerned with improving the resilience of the University. This means developing the University's ability to detect, prevent, minimise, and where necessary, deal with the impact of disruptive events or incidents. In the aftermath of an incident, business continuity enables the urgent and priority activities of the University to continue; in the longer term it will help the University to recover and return to "business as usual" as soon as possible while diminishing possible disruption.

1.3 The Business Continuity Management Framework has the following key objectives:

- To raise the profile of BCM within the University. This will include arrangements to make staff aware of plans, their roles in them and ensure they are trained appropriately.
- To identify urgent or priority (time critical) activities across the University and develop suitable business continuity arrangements for them.
- To establish defined structure to plan for and respond to incidents.
- To have on-going BCM arrangements at all levels and in all areas of the University that are subject to regular review, audits, and exercises.
- To develop and review the Framework for continuous improvement, with reference to best practice across the sector.
- To embed Business Continuity into the culture of the University so it becomes an integral part of decision making at all levels.

2.1 The scope of the Business Continuity Management Framework will operate across the University, covering all academic departments, professional services, subsidiary companies, and research units. The IT Department will remain responsible for specific IT Disaster Recovery

quickly it needs to be resumed and the impact if it is not available – on the safety of people, on the reputation of the University, its finances, and community.

2.4 The University has defined three types of business continuity situation, please also see the Decision Tree (Appendix 1) :

require the implementation of the [University's Critical Incident Plan](#), when they meet the plan's criteria for causing serious harm to staff, students, the University community, property, or its reputation. These situations may include, but are not limited to:

- Cyber security attack
- Fire
- Terrorist attack
- Significant property damage from flooding or other weather event
- Critical field trip incident or similar
- Mass casualty event either on campus or directly involving University community

The Critical Incident Plan is focused on the incident management phase and covers larger scale events posing immediate risk to individuals or property e.g. a national emergency, a power cut affecting the whole campus, etc. The Critical Incident Team would focus on the immediate response to the incident and in addition a business continuity response would be required in terms of how the University would continue its urgent activities which need to be recovered first.

If you believe there is a Critical Incident happening, you should call one of the following numbers:

IT Service Desk for potential Cyber Security/IT related matters
during normal working hours 01905 857500

Security for all other Critical Incidents and IT outside of
normal working hours 01905 855000

UEB, with advice from the University Secretary, will decide if the situation is a 'reportable event' to the Office for Students (OfS).

require escalation to the Vice Chancellor and University Executive Board (UEB). These situations are likely to involve the management of a range of significant situations which would not be identified as Critical Incidents (2.4.1) but do need to be managed and overseen at the highest level. These situations maybe identified as Major Business Continuity Situations due to their impact on: a significant cohort of students and/or staff; the academic provision of a course or school; wider student experience; day to day management of the University; financial sustainability and/or reputation of the University. These situations may

- 2.4.4 Please refer to the Business Continuity Decision Tree (Appendix 1) to assist in identifying the type of situation you are managing and how to escalate it appropriately.

The overall ownership and accountability for Business Continuity Management rests with the Vice Chancellor and the University Executive Board (UEB). The Vice Chancellor is accountable to the Board of Governors for the "organisation, direction and management of the University and leadership of the staff" (Articles 4.1.2)

Business continuity roles are separated into (i.e. pre-situation) roles and (during situation) roles. The organisational structure for Business Continuity operates at the Strategic, Tactical and Operational Levels.

In the event of a Critical Incident the management of that incident is in accordance with the Critical Incident Plan, recovery from the Critical Incident is managed by the Gold level group identified in this Policy.

The Audit Committee, on behalf of the Board of Governors, has a responsibility for ensuring that satisfactory arrangements are in place to ensure material adverse events, or reportable events, are managed appropriately.

As the senior decision-making group the UEB is responsible for:

- Oversight of the Business Continuity Management Framework, including the regular testing of the Critical Incident Plan.
- Oversight of the Business Continuity Management Policy.
- Oversight of post-incident/situation reviews, ensuring that lessons learnt during the incident/situation are taken forward appropriately and processes/systems improved.

- Ensuring that the Business Continuity Management Policy is kept up to date and communicated to the University community.
- Ensuring that the Critical Incident Plan and Business Continuity Management Framework are tested on a regular basis, areas for improvement identified and addressed
- Ensuring that post incident/situation reviews are undertaken by UEB (see Section 4).
- Reporting on the Business Continuity Management Framework and the state of readiness to UEB.
- Ensuring that any business continuity situations which are classed by the OfS as reportable events are reported to the OfS within the required time frame and records kept.
- Line management of the Business Continuity Officer.

The role of Business Continuity Officer (BCO) is undertaken by the University's Risk Management & Business Continuity Officer. They are responsible for co-ordinating the Business Continuity Management Framework. This involves:

- Raising the profile of Business Continuity across the University and ensuring that information is available to staff, with the aim of embedding BCM into the activities of the University.
- Providing advice and assistance throughout the BCM process.
- Developing appropriate templates for the University to detail its arrangements, ensuring consistency in the Framework with flexibility to recognise the differences across schools and professional departments.
- Supporting academic schools and professional departments in completing the relevant Business Continuity templates.
- Assisting in the development of overarching arrangements to support academic schools and professional departmental plans.
- Ensuring that the University's arrangements are regularly reviewed and tested.
- Monitoring the level of Business Continuity planning in the institution and reporting to the University Secretary, and in turn UEB, on this.
- Reviewing the BCM Framework to ensure it remains fit for purpose and to continuously improve the arrangements in place.
- Ensuring that all BCM arrangements work in tandem with the risk management framework.

It is important that everyone at the University is aware of the Business Continuity Management Framework. Staff should be aware of any arrangements in their department's business continuity plan including how they will be contacted/notified of an incident, whether or not they will be expected to work remotely, and where to access key information and updates.

In the event of an incident where a business continuity response is required the following will apply:

(

- 4.1 If there is a formalised response to a business continuity situation at the University then a post-disruption review will be undertaken by the UEB, with input from the Silver level group(s) and supported by the Business Continuity Officer, to ensure all lessons learnt from managing the business continuity situation are captured.
- 4.2 The Business Continuity Officer is responsible for documenting post incident reviews and working with the University Secretary to implement any identified improvements, reporting to UEB accordingly.

Business Continuity Management and Risk Management work closely together, as both are concerned with good governance and raising awareness about risks. However, the focus of the two areas is different; Business Continuity Management is only concerned with managing those threats or vulnerabilities that could cause a disruption to the University's operations, whereas Risk Management has a wider remit. The Risk Management and Business Continuity Officer works across both areas to ensure all risks and threats are identified and responded to accordingly.

Business Continuity Management may be used as a treatment of some risks identified in risk registers and is noted on the University's Strategic Risk Register. When developing business continuity arrangements, priority should be given to treating threats or vulnerabilities identified as most likely and having the greatest impact.

As part of the review and monitoring of the Framework Internal Audit has an important role in ensuring that the Business Continuity Management Framework achieves its objectives as set out in this document.

Information security covers the protection of all forms of information and is concerned with ensuring its confidentiality, availability, and integrity. A key part of the Business Continuity process focusses on protecting against a potential loss of resources, including essential information, thereby ensuring it is stored appropriately and remains available after a disruption. Information Security should be considered when developing alternative arrangements to store/access key information. The loss of university information – either by a loss of access to it or by someone else being able to access it – could have serious implications and dependent on the severity, would be classed as an incident at departmental level and also potentially for the University.

