Business Continuity Management Procedure	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Operations - Chief Operating Officer - Operations Committee
Associated Policy Statements:	N/A
Authorised Owner:	Business Continuity Manager
Authorised Co-ordinator:	Head of Governance
Effective date:	November 2022
Due date for full review:	November 2024
Sub documentation:	N/A

Approval History

Version	Reason for review	Approval Route	Date
1.0	First Draft	N/A	11/07
2.0	Second Draft	N/A	02/08
3.0	Final Draft	Executive Board	08/08
4.0	Update including audit recommendations	Executive Board	09/12
5.0	Review and Realignment to ISO22301:2012	Executive Board	10/14
6.0	Aligned to BCMS objectives	Continuity Steering Group	11/17
7.0	Update reflects changes to ISO22301:2019	Continuity Steering Group	08/20
8.0	Biannual review	Operations Committee	11/22

1. Purpose

Business Continuity Management (BCM)
(As defined in BS ISO 22301 – Business Continuity Management Systems – Requirements and Guidance:2019)

This is a business owned and business driven process that establishes a fit for purpose strategic and operational framework that:

- Proactively improves an organisation's resilience against the disruption of its ability to achieve key objectives.
- Provides a rehearsed method of restoring an organisation's ability to supply its key products and services to an agreed level within an agreed time of disruption.
- Delivers a proven capability to manage a business disruption and protect the organisation's reputation and brand.

This process is defined in ISO22301:2019 as a 'holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats if realized, might cause and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation brand and value-creating activities'

Compliance with ISO22301:2019

The University's BCMS will be in line with the procedures and guidance as defined within ISO standard 22301:2019 as agreed by the Executive Board. The application and implementation of the plan will be tailored to suit the environment and business relating to higher education to achieve an efficient and flexible system that can be readily updated and where ownership of the information is within the faculties and departments whose plans contribute to the University's overall plan.

1.1. Provide a framework for the development of a robust and consistent BCMS throughout the University, supporting the University in meeting a wide range of legal and regulatory requirements.
1.2. Complement the University Risk Management Framework by identifying and planning for, high impact scenarios, where BCM is the appropriate risk mitigation strategy. Align risk management disciplines and drive organisational resilience.
1.3. Ensure that the BCMS provides planning, processes, training, and continuous improvement to manage operational incidents throughout the University. Provide a framework of management and decision making at a time of immense pressure that will result in an agreed recovery program that has minimised the impact of the event.
1.4. Formalise critical corporate service priorities, and minimum service levels, during times of disruption and prepare services to manage the consequences of disruptive events.
1.5. Ensure that critical processes and resources are recovered in the event of major disruption before their non-performance threatens the long-term survival of part, or all, of the University.
1.6. Identify and mitigate business continuity risk. Enhance service performance and delivery by understanding dependencies and associated risks, including supply chain resilience. Comply with good practice to minimize the exposure of the organisation to claims.
1.7. Promote and maintain the reputation of the University.
1.8. Align to the requirements of ISO 22301:2019 guidelines.
1.9. Promote a resilience culture embedded in strategy, management systems, change control, annual business planning, key performance indicators (KPI), training and in values and behavior.

Key Targets

In the event of a significant business disruption, the University will aim to:

- Identify and reallocate alternative teaching and research space within 48 hours of loss.
- Following the loss of a student residence, residents will be directed/moved to a planned, short-term place of safety within 2 hours and be assisted in finding shelter by nightfall.
- Have the Incident Response Team (bronze) on site within 1 hour.
- Have the Incident Management Team (silver) assembled on site within 1.5 hours of escalation or declared as a serious or critical incident by the President & Vice Chancellor / Silver Commander
- Disseminate information/instructions to students and staff within a reasonable time of an incident affecting the site.
- Have the web site and email available within 1 day.
- Direct staff, students and management to access regular, up to date information on the web site following an incident
- Contact staff regarding alternative working space within 2 days.
- The requirement for alternative office space will vary due to the nature and scale of the incident together with the priority and nature of the work to be carried out (e.g., front/back office). For services considered high priority/essential we will aim to make office space available within 7 days - 14 days dependent on power and data provisions
- The priority for space will be judged primarily on health and safety grounds followed by business impact and the alternative options available.
- Students will be contacted by Faculty/Registry regarding building availability/alternative teaching space and alternative timetabling .
- Maintain ability to provide alternative food sources in the event of one or more catering facilities being unavailable.
- Ensure safe working environment for all staff and students.

2. Scope and Exceptions to the Procedure

The BCM system focuses on the development of business continuity arrangements for the University to respond to disruptions, using a risk-based approach. The programme covers services across all faculties and departments, Central Support Services and Traded Services.

2.1. The following areas are all within the scope of the BCMS:

- Faculties and Professional Services Directorates
- University owned, operated, maintained, and insured buildings including Research Park business incubator units
- Supply chain: strategic and business critical item suppliers, contracts, and maintenance arrangements
- Surrey Sports Park (SSP)
- Commercial service provision e.g., Redbridge University Procurement Services; Defra Animal Surveillance
- Satellite sites including provision of management support to the China Campus

2.2. Exclusions from scope:

Where we own the buildings but do not run the services or hold responsibility for managing business interruption. A comprehensive list is held on the Tenanted Estate Terrier database. Examples include:

- Research Park
- AQA / BBC Surrey
- Staff Nursery / Harlequins Training Centre

- International House, Bellerby Court
- UCAS / Examination board procedures
- Private residential properties used by students
- Students' Union Societies
- Workplace and Business placements for students
- Local Resilience Forum Partner plans

3. Definitions and Terminology

BCM – Business Continuity Management
BIA – Business Impact Analysis
IMP – Incident Management Plan
IRT – Incident Response Team
IMT – Incident Management Team
SMT – Strategic Management Team
MAO - Maximum Acceptable Outage – time it would take for adverse impacts, which might arise because of not providing a product /service or performing an activity, to become unacceptable.
MTPD - Maximum Tolerable Period of Disruption – time it would take for adverse impacts, which might arise because of not providing a product /service or performing an activity, to become unacceptable.
MBCO - Minimum Business Continuity Objective – minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption.
MAA - Mutual Aid Agreement – pre-arranged understanding between two or more entities to render assistance to each other.
RPO - Recovery Point Objective - point to which information used by an activity must be restored to enable the activity to operate on resumption (also known as maximum data loss).
RTO - Recovery Time Objective – period following an incident within which Product or service must be resumed, or Activity must be resumed, or Resources must be resumed.

4. Procedural Principles

This Procedure sets out the principles and core responsibilities for Business Continuity Planning (BCP) in the University of Surrey.

4.1. Strategic

- Business Continuity addresses risks and issues which may jeopardise the quality of the University's academic provision and its reputation, its financial provision and legal position (including environmental impact).
- The University will develop and maintain a comprehensive suite of BCPs aligned to meet the requirements of ISO 22301:2019.
- The BCPs will aim to protect key and mission critical activities and enable the University to continue to operate following a major disruption to activity at a predetermined level of operation
- It is intended to resume normal business practice whenever possible unless this is overridden specifically at President & Vice Chancellor level.
- The President & Vice Chancellor, or designate, will decide when a situation presenting a possible reputation risk should be deemed an emergency and is responsible for managing the situation.
- A key principle of ISO 22301:2019 is that of continual improvement through the implementation of the 4 elements of the Business Continuity Life Cycle. The level of Business Continuity Management Planning maturity sought by the University will be risk

based and the development monitored through an appropriate reporting mechanism to the Executive Board.

4.2. Process

- A formal Business Impact Analysis will be undertaken to identify and determine the requirements of the University.
- The BCP will be reviewed annually as a whole, and individual plans as required following the occurrence of an incident that affected normal operations or identified areas not previously considered.
- The BCP will be required to be tested on an annual basis by undertaking a desktop exercise facilitated by the Business Continuity Manager. Where Departments / Faculties do not complete the exercise testing of their plans, a non-compliance report will be compiled and shared at the next Business Continuity Steering Group (BCSG) meeting.
- In respect of physical emergencies, appropriate members of the Incident Response Team shall be called in by the Security Manager (On Call) where a situation develops which cannot be managed through normal business practices.
- The duty manager will alert the relevant Silver Commander who, where required will convene the Incident Management Team (IMT). Alternatively, the IMT may be convened at the request of the President & Vice Chancellor on the advice of key University officers following existing management escalation processes. Advice may also be sought from outside agencies, for example, the emergency services.
- The essential test shall be that it is the view that normal operational arrangements are incapable of being augmented or re-prioritised, to prevent an escalating risk becoming an incident or major business interruption without exceptional action being taken, usually involving the provision of significant additional resources.
- The membership of the IMT shall be decided by its chair in the light of the circumstances. All senior officers of the University or their designated deputies shall be approached as required to serve on the IMT.
- All internal and external communications during an incident shall be the responsibility of a core team of professional staff including the Director of Communications & Public Affairs, Chief People Officer, Head of Security, Chief Student Officer, President & Vice Chancellor, and Health Professional or designated Deputies as appropriate.
- The Business Continuity Plan(s) will address both general management aspects of the continuity process as well as those for specific IT and voice/data communications elements, and record which are the responsibility of the Chief Information & Digital Officer (CIDO), and which are the responsibility of the School/Department concerned.

4.3. People

- All responsible staff will be aware of their BC responsibilities and trained appropriately.
- The Directorate or Faculty Head should in their points of contact per BCP, select nominated deputies, and have sufficient cover to deal with the situation should they not be available.
- Identified Business Continuity Representatives in Faculties and Departments are to assist in the completion of a Business Impact Analysis and Business Continuity Plans. They must manage, accept, or plan for identified risks in their areas of responsibility including carrying out the annual review and update. They are expected to encourage the active participation of staff in business continuity issues including advice on, and participation in appropriate tests.
- The Security Department are responsible for the update and circulation of contact details for all key officers and designates who can be considered likely to be required to serve on the Incident Management Team, and to circulate this information periodically to the same group of individuals.

4.4. General Information

A key distinction is made between 'physical emergencies', such as fires, cases of a communicable disease and death where a particular event or events require a response to be made following other than normal business practice, and situations which occur which have the potential to damage the University's brand and reputation. Examples of the latter include recruitment and retention problems, external funding problems and overseas operational problems. The Chief Operating Officer (through the Director of Campus Services) is responsible for the overall development of the University's Business Continuity Plan(s) process, including the Incident Management Plan, and for testing of threat specific and consequence management plans. Business Continuity Plan(s) will be developed with, and held by, Departments and Schools as appropriate.

4.5. Business Impact Analysis

This will be carried out by each Faculty and Directorate to identify the following:

- The critical processes carried out in each location
- The critical events associated with the processes
- The critical technology (applications and software)
- The critical databases
- Faculty/business unit/department owned servers supporting the above
- Specialist space (location)
- Vital paper records
- External dependencies (external suppliers and contacts)
- Specialist equipment
- Internal dependencies
- Associated business risks

The results will be analysed to identify

- Focus of business continuity plans
- Any single points of failure
- Unique business continuity issues that apply to a specific area/activity
- Investment required to protect this
- Level of risk being accepted

4.6. Business Continuity Plans

The critical processes identified in the BIA's of each department will guide the development of the required business continuity plans by considering appropriate mitigation strategies to assist in case of business interruption.

4.7. The University Incident Management Plan

The University of Surrey Incident Management Plan (IMP) will be comprised of a suite of documents developed to manage the continuity of critical processes.

The preparation review and update of the key high-level plans (shown below) is managed centrally and is the responsibility of Chief Operating Officer and appointed team who provide the direction, outline, planning, training, testing, and reporting of the BCM.

The Incident Management Plan is supported by a suite of threat specific and consequence management plans, in addition to building specific (hazard) plans and service BCPs, as set out in the BCMS Programme Overview.

The responsibility for preparation, review, and update of these plans' rests with the plan owners (Faculty Dean/Head of Department/ Head of Service).

These documents will be stored in several places and in a variety of methods to ensure they are accessible in a time of need:

- Electronically on IT Services managed servers

- Electronically and in hard copy format by each Faculty and Directorate
- On the Business Continuity SharePoint Site

4.8. Business Recovery

The University will have sufficient information under the umbrella of its BCM plans to execute an efficient recovery after an incident to minimize the overall impact of any event. An incident which has affected its physical resources will provide the University with options regarding its reinstatement. A full review of the impact of the loss will be undertaken with an evaluation of the business recovery programme before decision is made to proceed with major reinstatement works.

The resources to manage this stage of the process will be drawn from those managers who may have been initially involved in the Incident Management Team and the management of business continuity. These staff will move to business recovery planning and implementation at the appropriate time to progress an efficient return to the agreed full service.

The standard allows for a full evaluation with detailed planning focused on the specific issues to be undertaken to ensure an appropriate recovery strategy.

5. Governance Requirements

5.1. **Implementation: Communication Plan**

The Executive Board has overarching responsibility for this Procedure and its implementation. The responsibility for the development of the University of Surrey BCMP is delegated to the Chief Operating Officer, Directorate of Campus Services, Head of Security, and the Business Continuity Manager. Along with the management of the overarching plans this also includes responsibilities for the testing and review, and monitoring/reporting of progress, format revisions training events and annual testing. The responsibility and accountability for Faculty and Directorate level plans rests with the relevant Faculty Dean or Directorate. Any non-compliance for plan refresh or testing not completed as per requirement, should be escalated to the Business Continuity Steering Group, with recommendations to complete within one calendar month of the BCSG meeting. An update of outstanding or overdue activities will be provided to the Department Head, should the updates not be undertaken, the BC Manager to raise non-compliant report to the Chief Operating Officer / BCSG.

5.2. **Implementation: Training Plan**

To be communicated via local inductions and the mandatory introduction to Business Continuity Training (targeted at Vice President, Executive Deans, Senior Management, Faculty Managers, along with Plan Authors). Colleagues with business continuity responsibilities will be required to undertake the e-learning training to confirm their understanding with a completion statement. Where training is not completed, will be logged, and shared with the Business Continuity Steering Group.

Each operating Faculty and Directorate will develop and provide to the Director of Campus Services:

- Copies of plans/updated plans
- Positive assurances that the plans reflect current activities and risk
- Approved (signed off) plans by the relevant Head of Department and where applicable the Dean.

The plans/updated plans will be provided annually to ensure the plans are in line with the academic year

5.3. **Review:**
The procedure is to be reviewed on a biannual basis, unless to due a major incident or fundamental change with within the organisation's procedures, processes, or regulatory review.

5.4. **Legislative Context and Higher Education Sector Guidance or Requirements**
The influence on the University of Surrey is to attain an ISO 22301 Business Continuity Management System (BCMS) international standard accreditation designed to protect the business from potential disruption. This includes weather, fire, flood, natural disaster, IT outage, terrorism, or pandemic. The management system allows higher education establishments to identify threats that are relevant to the business and the critical functions it may impact and allows the university to put plans in place ahead of time to ensure that the business does not come to a standstill and return to business as usual within required timeframes.

5.5. **Sustainability**
This procedure has no impact on carbon emissions or on energy consumption.

6. Stakeholder Engagement and Equality Impact Assessment

6.1. An Equality Impact Assessment was completed on 26/09/2022 and is held by the Authorised Co-ordinator.
6.2. Stakeholder Consultation was completed, as follows:

Stakeholder	Nature of Engagement	Date	Name of Contact
Governance	Procedure review	27/10/2022	Andrea Langley
H&S	Procedure review	21/09/2022	Matt Purcell
CIDO	Procedure review	06/09/2022	Ambrose Neville
Security Services	Procedure review	08/09/2022	Mark Chatterton