

Business Continuity Management Policy

Operational Owner:	Justin Cuckow, Business Continuity Manager
Executive Owner:	David Sharkey, Chief Operating Officer
Implementation date:	December 2017
Date of next review:	December 2019
Related policies:	Flexible Working Policy On call policy Acceptable Use of IT
Policy History:	Updated policy to reflect ISO22301:2012 requirements and revised BCMS scope and exclusions

Version History

Version	Author	Revisions Made	Date
1	A Lawson	First Draft	November 2007
2	A Lawson	Second Draft	February 2008
3	A Lawson	Final	August 2008
4	A Lawson	Update including Audit recommendations	September 2012
5	A Lawson	Review and Realignment to ISO22301:2012	October 2014
6	J Cuckow	Further aligned to BCMS objectives / scope (no significant changes to content/meaning)	November 2017

Approval History

Equality Analysis

Version	Reviewed by	Comments	Date
1	Equality & Diversity Jo McCarthy-Holland	No negative impact on equality identified	27.11.2017

Committee Sign Off

Version	Committee Name	Date of Final Sign Off
3	Executive Board	August 2008
4	Executive Board	September 2012
6	BC Steering Group	December 2017

1	<p>Introduction</p>
	<p>Business Continuity Management (BCM) (As defined in BS ISO 22301 Societal security – Business Continuity Management Systems - Requirements and Guidance:2012)</p> <p>This is a business owned and business driven process that establishes a fit for purpose strategic and operational framework that;</p> <ul style="list-style-type: none"> • Proactively improves an organisations resilience against the disruption of its ability to achieve key objectives • Provides a rehearsed method of restoring an organisations ability to supply its key products and services to an agreed level within an agreed time after a disruption and • Delivers a proven capability to manage a business disruption and protect the organisations reputation and brand <p>This process is defined in ISO22301:2012 as a <i>‘holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of it key stakeholders, reputation brand and value –creating activities’</i></p> <p>Compliance with ISO22301:2012</p> <p>The university’s BCMS will be in line with the procedures and guidance as defined within ISO standard 22301:2012 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 in order 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.</p>
1.1	<p>Purpose</p>
1.1.1	<p>BCM Aims</p> <ul style="list-style-type: none"> • 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. • 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. • 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.

- Formalise critical corporate service priorities and minimum service levels during times of disruption, and prepare services to manage the consequences of disruptive events.
- 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.
- 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.
- Support the successful delivery of the University Corporate Strategy 17-22.
- Promote and maintain the reputation of the University.
- Align to the requirements of ISO 22301:2012 societal security guidelines.
- Promote a resilience culture embedded in strategy, management systems, change control, annual business planning, KPIs, training and in values and behaviour.

Key Targets

In the event of a significant business disruption we aim to:

1. Identify and reallocate alternative teaching space and research space within 48 hours of loss
2. 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
3. The Incident Response Team (bronze) will be on site within 1 hour
4. The Incident Management Team (silver) will be assembled on site within 1.5 hours of escalation or declared a serious or critical incident by the President & Vice Chancellor / Silver Commander
5. Aim to disseminate information/instructions to students and staff within a reasonable time of an incident affecting the site
6. Web site and email available within 1 day
7. That staff, students and management are directed to access regular up to date information on the web site following an incident
8. Staff will be contacted regarding alternative working space within 2 days
9. 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 dependant on power and data provisions
10. The priority for space will be judged primarily on health and safety grounds followed by business impact and the alternative options available.
11. Students will be contacted by Faculty/Registry regarding building availability/alternative teaching space and alternative timetabling

	<p>12. Maintain ability to provide alternative food sources in the event of one or more catering facilities being unavailable</p> <p>13. Ensure safe working environment for all staff and students</p>
1.2	Scope
1.2.1	<p>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.</p> <p>The following areas are all within the scope of the BCMS:</p> <ul style="list-style-type: none"> ◇ Faculties and Central Support Services ◇ University owned, operated, maintained and insured buildings <ul style="list-style-type: none"> ○ Including Research Park business incubator units ◇ Supply chain: strategic and business critical item suppliers, contracts and maintenance arrangements ◇ Traded services e.g. Robens, Surrey Sports Park ◇ Commercial service provision e.g. Redbridge University procurement services; Defra Animal Surveillance ◇ Satellite sites including provision of management support to the China Campus <p>Exclusions from scope</p> <ul style="list-style-type: none"> ◇ 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: <ul style="list-style-type: none"> ○ Research Park ○ AQA / BBC Surrey ○ Staff Nursery / Harlequins training centre ○ Millennium & International House, Bellerby Court ◇ UCAS / Examination board procedures ◇ Private residential properties used by students ◇ Student Union Societies ◇ Workplace and Business placements for students ◇ Local Resilience Forum Partner plans
1.3	Equality Analysis
1.3.1	<p>The University is strongly committed to equality of opportunity and the promotion of diversity for the benefit of all members of the University community. The University's approach is to promote equality across the full range of its activities, in employment, teaching and learning and as a partner working with and within local, national and international communities. Equality Analysis is a process which examines how the impact of the policy has been considered on the diverse characteristics and needs of everyone it affects. This policy has been reviewed and no negative impact on equality has been identified.</p>
1.4	Terms and Definitions
	<p>Business Continuity Management (BCM)</p> <p>BCM – Business Continuity Management</p> <p>BIA – Business Impact Analysis</p>

	<p>IMP – Incident Management Plan</p> <p>IRT – Incident Response Team</p> <p>IMT – Incident Management Team</p> <p>SMT – Strategic Management Team</p> <p>MAO - Maximum Acceptable Outage – time it would take for adverse impacts, which might arise as a result of not providing a product /service or performing an activity, to become unacceptable</p> <p>MTPD - Maximum tolerable period of disruption – time it would take for adverse impacts, which might arise as a result of not providing a product /service or performing an activity, to become unacceptable</p> <p>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</p> <p>MAA - Mutual Aid agreement – pre-arranged understanding between two or more entities to render assistance to each other</p> <p>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)</p> <p>RTO - Recovery time objective – period of time following an incident within which Product or service must be resumed, or Activity must be resumed, or Resources must be resumed</p>
1.5	Legislative context
	<p>Risk assessment</p> <p>The University has an established risk management process. High level risks are identified and reviewed at strategic level The risk assessment for business continuity is identified in the BIA’s and these risks are reviewed for possible inclusion in the Faculty/Departmental risk registers as appropriate. Mitigation for the risks identified in the BIA’s is covered in Faculty /Departmental Business Continuity Plans.</p>
1.6	Health & Safety Implications
	<p>The health and safety of incident responders is of vital importance. The University will ensure that any incident is managed closely to ensure full compliance with license conditions and the health, safety and wellbeing of staff, students, visitors and contractors. Post incident support will be made available to support wellbeing as appropriate. The Health and Safety department play an important role in providing information and advice in support of the management of incidents and in liaising with emergency services.</p>
2	Policy
2.1	Principles
	<p>This Policy Statement sets out the principles and core responsibilities for Business Continuity Planning (BCP) in the University of Surrey</p> <p>Strategic</p>

- 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 22301:2012
- 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 22301:2012 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.

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 tested against an exercise programme and the reports will be compiled.
- 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 Acting 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 particular 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 Marketing and Communications, Vice - President, Human Resources, Head of Security, Registrar, 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 IT Director and which are the responsibility of the school/department concerned.

	<p>People</p> <ul style="list-style-type: none"> - All responsible staff will be aware of their BC responsibilities and trained appropriately - Staff will discharge their normal responsibilities in response to events although they may be required to re-prioritise or fill in for absent employees if necessary. - 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 their 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. <p>General Information</p> <ul style="list-style-type: none"> - 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 Business Continuity Manager) 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.
2.2	Procedures
2.2.1	<p>Business Impact Analysis</p> <p>This will be carried out by each Faculty and Department to identify the following;</p> <ul style="list-style-type: none"> • 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 <p>Results analysed to identify</p> <ul style="list-style-type: none"> • 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

<p>2.2.2</p>	<ul style="list-style-type: none"> • Level of risk being accepted <p>The University Incident Management Plan</p> <p>The University of Surrey Incident Management Plan (IMP) will comprise of a suite of documents developed to manage the continuity of critical processes.</p> <p>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</p> <p>The University 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.</p> <p>The responsibility for preparation, review and update of these plans rests with the plan owners (Faculty Dean/Head of Department/ Head of Service)</p> <p>These documents will be stored in a number of places and in a variety of methods to ensure they are accessible in the time of need</p> <ul style="list-style-type: none"> • electronically on IT Services managed servers • electronically and in hard copy format by each faculty and department • on the Business Continuity SharePoint Site <p>Business Continuity Plans</p> <p>The critical processes identified in the BIA’s the department will guide the development of the required business continuity plans by considering appropriate mitigation strategies to assist in case of business interruption.</p> <p>Business Recovery</p> <p>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 program before decision is made to proceed with major reinstatement works.</p> <p>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.</p> <p>The standard allows for a full evaluation with detailed planning focused on the specific issues to be undertaken to ensure an appropriate recovery strategy.</p>

3	Governance & Directory Requirements
3.1	Responsibility
	<p>The Executive Board has overarching responsibility for the Policy and the implementation. The responsibility for the development of the University of Surrey BCMP is delegated to Chief Operating Officer, Deputy Director of Estates, Head of Security and BC Manager. Along with the management of the overarching plans this also includes responsibilities for the and review, and monitoring/reporting of progress, format revisions training events and annual testing</p> <p>The Responsibility and accountability for Faculty and Departmental level plans rests with the relevant Faculty Dean or Head of Department.</p> <p>Each operating Faculty and Department will develop and provide to the Business Continuity Manager</p> <ul style="list-style-type: none"> - 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 by 31 July annually to ensure the plans are in line with the academic year.
3.2	Implementation / Communication Plan
3.2.1	To be communicated via local induction and via the Mandatory Introduction to Business Continuity Training (targeted at Senior managers: Executive Deans, Faculty Managers, Vice Presidents, Directors and Deputy Directors along with plan authors: heads of department / schools and heads of service / function managers) and internal champions network. The organisational resilience campaign will also promote the principles, procedures and governance.
3.3	Exceptions to this Policy
	There are no other exceptions to this policy unless formal documented approval has been provided by the COO or their appointed deputy and brought to the BC Steering Group.
3.4	Supporting documentation
	N.B. Supporting documents have restricted access and are held centrally on SharePoint in addition to being held locally in Faculties and Departments.