INCIDENT AND BUSINESS CONTINUITY MANAGEMENT POLICY

INTRODUCTION

1.1 Purpose of the policy

This policy has been designed to ensure that Keele University has a framework in place to manage incidents and ensure business continuity in the event of a disruptive incident. The policy outlines how incidents will be managed, how the level of management response to an incident is determined, how we will formalise the use of a business continuity management framework to inform our approach to incident management, and new arrangements to support and oversee policy development, implementation and review.

1.2 What is an incident?

A large range of matters may constitute an incident. The general working definition to be used in this policy is: *an incident, or threat of one, that risks major disruption or damage to the University community.* These may be rapid in onset and develop quickly with immediate effects; or be so-called 'rising tide' incidents which will develop over days, weeks or even months and the impact of which may not be apparent within the early stages.

1.3 What is business continuity?

Business continuity is defined as: *the concept that key functions and critical activities carried out by the University remain deliverable in the event of a business disruption.* Business continuity involves implementing whatever plans are required, within measurable timeframes, that are necessary for the University to continue with its key functions and critical activities. These may span from actions which return us to business-as-usual within hours (e.g. disruption due to bad weather), days (e.g. an overseas evacuation), months (e.g. the loss of laboratory facilities) or even years (e.g. due to a national lock-down to control the impact of a global pandemic).

1.4 The scope of incidents to be considered

Incident management and business continuity may relate to: the physical estate and its services (our **PREMISES**); staff, students, visitors, and other people both on and off campus in the UK and anywhere in the world (our **PEOPLE**); our digital services and underpinning business infrastructures (our **PROCESSES**); our suppliers and partners (our **PROVIDERS**); and/or our brand and reputation (our **PROFILE**); or combinations of them.

1.5 The stages of incident and business continuity management

The University's protocol and plan will follow the following five stages of incident management and business continuity:

1. **Horizon Scanning/Monitoring Period**: When there is an early detection of a potential incident issue, but not yet presenting a direct or indirect risk to the University;

2. **Identification of Risk/At Risk Period**: When there is evidence of a risk of incident that could start to have an impact on the University;

3. **Incident Period**: When there is evidence of a direct impact and possible identification of a significant disruptive event(s) being experienced by the University and the need to use a business continuity management framework to inform plans;

4. **Post Incident Period**: When the immediate threat or incident has been resolved and the University is recovering (managing/returning back to business-as-usual status) informed by a business continuity management framework; and

5. **Review Period**: When the incident id over and business continuity plans delivered a return to business-as-usual.

1.5 How the policy is informed

All aspects of incident management and business continuity at the University aim to align with the Business Continuity Institute's (BCI) *Good Practice Guide* and are aligned to the relevant International Organisation for Standardisation (ISO) technical standards, British Standard (BS) EN ISO 22320:2018 *Security and resilience – Emergency management – guidelines for incident management* and *BS EN ISO 22301:2019 Security and Resilience - Business continuity management systems - Requirements.* These documents provide the framework for the implementation of incident and business continuity management across the University.

1.6 Section of the policy

This policy is divided into the following parts:

Part A: MANAGEMENT RESPONSIBILITIES and ESCALATION

Part B: PROTOCOLS and PLANS

Part C: BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

Part D: IMPLEMENTATION, MONITORING, GOVERNANCE and PUBLICATION

Part E: POLICY EFFECTIVENESS and REVIEW

Part F: TRAINING and INFORMATION

Part A: MANAGEMENT RESPONSIBILITIES and ESCALATION

2.1 The Chief Operating Officer is responsible for this policy and arrangements, supported by an Incident and Business Continuity Manager (to be appointed). Incidents are managed through an incident management command structure, using an established and widely used approach for managing the response to, and recovery from incidents and ensuring business continuity.

2.2 The command structure builds from one to up to three levels of management response. The levels of response are incremental and additive. Response levels build. They are not replaced. **The appropriate level of response can be determined using a dynamic risk assessment** (Annex 1) to establish if incidents pose low, moderate, or high risk of impact to business continuity. This in turn can inform the appropriate command level to manage a risk. The command levels are:

- **Bronze (low risk):** The **operational** level of a response, led by those areas appropriately skilled and trained to address the specific issues being presented by the incident – usually as part of a core service function (e.g., student services, estates, security, communications, IT, lab managers/technical staff, faculty operations). This may include specific professional services and areas and/or role and responsibilities held by schools and faculties. This may include the provision of out-of-hours arrangements (e.g., on-call trades people, out-of-hours student support, crisis communications and/or those responsible for management of specialist equipment). A bronze level response would include the usual level of collaboration across professional service areas and with academic areas, as would reasonably be anticipated under business-as-usual arrangements. The bronze level response will be led by an operational lead dictated as most appropriate to the nature of the matter and the required response (e.g., a student welfare matter will be led by the Directorate of Student Services and Success). **Heads of Professional Service areas and Heads of School/Heads of Faculty Operations deliver this level of response and Directors of Professional Services and Executive Deans carry the management responsibility for ensuring this level of response is operational at the time of the incident and in readiness of it.** Most incidents will be managed via business-as-usual bronze level responses and would be considered **low risk** (Annex 1) to business continuity.

- **Silver (moderate risk):** The **tactical** level of response, recognising the requirement for management of incidents and their impacts to business continuity which may require a level of additional management oversight and co-ordination beyond that provided by business-as-usual responsibilities executed via a bronze level of response. This level of response is led by (or on behalf of) the Chief Operating Officer and the aim of this level of response is to oversee effective co-ordination and engagement across and between several different areas of the University and may include engagement with external agencies (e.g., Public Health England, Environment Agency, Joint Information Systems Committee (JISC), relevant emergency service(s)). This level of response may require the formation of an Incident Management Group (see below). **The Chief Operating Officer carries the management responsibility for ensuring this level of response is in place and they may directly manage this level of response.** This additional level of response would be required for incidents posing **moderate risks** (Annex 1) to business continuity.

- **Gold (High risk):** The **strategic** level of response provides University-wide oversight and co-ordination of the most serious of incidents and impacts on business continuity. It also takes a specific lead on significant strategic risk of reputational damage. **This level of responsibility resides with the Vice Chancellor and Deputy Vice Chancellor and Provost.** This additional level of response would be required for incidents posing **high risks** (Annex 1) to major disruption to business continuity.

Table 1 outlines the above three levels of response, the nature of the level of response and some (non-prescriptive) selected examples of incidents which might lead to a requirement to be managed under the three different levels of command.

Table 1: Summary of command level responses with some examples of incidents which might necessitate management at this level of the command structure.

Response	Risk	Approach	Operational response	Management Responsibility	Examples of incidents
BRONZE	LOW	Operational	One or more operational teams acting within established business as usual approaches including out of hours on call arrangements. This may also include engagement with external agencies. A single level of command response via business as usual arrangements.	Directors of Professional Services or Executive Deans are responsible for ensuring business-as-usual management arrangements are in place to deliver this kind of response.	• Equipment failure • A student in mental health crisis • Urgent press statement • IT system down • A flooded office • A minor accident to a student/member of staff • A student being detained at a UK boarder • Storm damage • Theft from a building
SILVER	MEDIUM	Tactical	Co-ordination and oversight of several operational responses led by different areas of the University both during working periods and out of hours. This may also include engagement with external agencies. A level of response required at both bronze and silver command levels.	Chief Operating Officer is responsible for ensuring arrangements for the management of incidents and business continuity measures are deployed via development and delivery of the policy.	• IT failure to parts of campus • Prolonged loss of power • Student/staff death in suspicious circumstances • Student diagnosed with meningitis • Major Fire/Flood • Major Travel disruption • Major gas leak • Widespread infection • A large-scale food poisoning • A radioactive leak • Death of a visitor on campus • Terrorist attack off campus • Overseas large-scale natural disaster
GOLD	HIGH	Strategic	Oversight of the most significant incidents and impacts to business continuity including risks of institution-level operational failure or major reputational risks. Bronze, silver and gold command levels are required.	The Vice Chancellor is responsible to Council for ensuring appropriate incident management and business continuity approaches are in place and for oversight of the most serious of incidents and impacts to business continuity.	• Major loss of facilities and/or buildings • Lack of operational continuity to all campus • Campus wide Cyber or ransomware attack • Accidents with significant injuries/deaths • Terrorist attack on campus • Global pandemic requiring lockdown

2.3 Escalation to higher levels of command response

Incidents that create risks or require business continuity measures identified as moderate risk, which cannot be managed or delivered by business-as-usual (bronze level/low risk) response should be escalated to include a silver level response. This happens when:

- The bronze level response considers that the risks and disruption of key functions associated with the incident cannot be effectively managed within the resources, authority and expertise levels at their disposal;

- When the level of risk to business continuity arising from the incident meets the level where escalation is appropriate (moderate level of risk);

- Concerns are raised that matters are not being escalated and should be;

- When co-ordination across a number of areas is required and not possible or effective to achieve via business-as-usual collaborative approaches;

- On the decision of the Professional Services Director or Executive Dean responsible for one or more of the areas providing the bronze level response, or the Chief Operating Officer.

2.4 Incidents which cannot be managed by a silver level response alone, are escalated to include gold level response. This happens when:

- When co-ordination across a significant number of areas is required and not possible to achieve via business-as-usual collaborative approaches;

- Concerns are raised that matters are not being escalated and should be;

- On the decision of the Chief Operating Officer, Vice Chancellor and/or Deputy Vice Chancellor and Provost.

Part B: PROTOCOLS and PLANS

3.1 This section outlines protocols which can support incident and business continuity management, to support the command structure in the management of incidents and business continuity. This covers management arrangement both during the working week and out of hours.

3.2 **Bronze level management response protocols:** Local protocols/plans exist to deal with a wide range of specific type of incidents. These guide the bronze level (business-as-usual) response. Current bronze level response protocols/plans include:

- Fire incident management
- Serious Crime incident
- Flood incident
- Communicable diseases management
- Terrorist incidents
- Student Accommodation emergencies
- Off campus incident management
- Unexpected death of student or staff members
- Pandemic disease measures
- Environment incident management plans
- Cyber and ransomware attack

Some of these protocols/plans also provide for an approach to escalation to a Silver level of response detailed in this policy.

Responsibility for ensuring the above protocols/plans are in place and effective which rests with a number of professional service directors. Assurance as the presence and effectiveness of these plans and the identification/management of co-ordinated and collaborated protocols/plans across Directorates and Faculties should be provided by the Incident and Business Continuity Management Group (IBCMG) supported by the Incident and Business Continuity Manager. The purpose and responsibilities of the IBCMG and the Incident and Business Continuity Manager role are outlined in **Part D**.

3.3 Initial reporting of a potential incident

The significant majority (but not all) potential incidents will be initially reported to or via the Campus Safety Team (24 hours a day, 365 days a year). They will:

1. Liaise with the Campus Safety Team Supervisor to consider the appropriate response.
2. If then appropriate, notify the appropriate area to lead a bronze level response (in and out-of-hours) or continue to handle the matter directly: a) If the incident is clearly an incident which is a Campus Safety related matter; b) If agreed by the relevant bronze lead or silver level response; or c) If requested by the appropriate bronze or silver level response whilst they mobilise/escalate.
3. Register the commencement of a potential incident.

At this stage the matter would be considered as within the business-as-usual operations of the University, including any established out-of-hours arrangements. An incident would not be considered to exist at this point.

3.4 Although an incident may be initially reported to the Campus Safety Team, where appropriate, the Campus Safety Lead (Supervisor, Head of Campus Safety or Campus Safety Team Operations Manager) will transfer responsibility of the incident to the most appropriate area within the University for e.g., a student welfare matter would be referred to the Directorate of Student Services and Success and an IT matter to the Directorate of Information and Digital Services. At this point, decision will be made on the requirement for the Campus Safety Team but it may be mutually agreed that the Campus Safety Team still remains as the main contact with the emergency service(s) in such relevant circumstances.

3.5 Liaison with Emergency Services

3.5.1 Where incidents involve a risk or threat to life or serious injury, serious damage or loss of infrastructure, serious crime or disorder, or pose a risk to the wider community, then it is likely that the Emergency Services will need to play a key role in responding and managing these risks. If an emergency situation is occurring, then under normal circumstances the individual first becoming aware of this should notify the appropriate Emergency Service(s) via 999. They should then notify the Campus Safety Team who will confirm that Emergency

Service(s) are aware. The Campus Safety Team staff will likely be deployed to respond to the incident at the direction of the supervisor/senior duty officer.

3.5.2 When the Emergency Service(s) arrive, they will assume primacy over the operational response to the specific risk or threat. Under these circumstances, they are likely to request support from the University, the nature of which will depend on the incident. This co-ordination will normally be managed through the Campus Safety Team. In addition, it is likely that the University will have its own priorities and considerations that fall outside of the primary focus of the Emergency Services, including business continuity measures.

3.5.3 Under these circumstances where an immediate response is required, the Campus Safety Team Supervisor or Deputy will normally take control and operate as bronze level response.

3.5.4 The Campus Safety Team bronze level response will manage the initial phase of the incident and, if and when appropriate, request a silver level of response from the Chief Operating Officer. They will confirm their management lead for the silver level response (either directly or via a delegation) who leads co-ordination of a response. They may also consider the on-going bronze level response as adequate and not requiring of a silver level response.

3.6 Silver and Gold Level command protocols

These levels of response may, where appropriate use one or more of the following:

- A framework to carry out a **dynamic risk assessment** (Annex 1)
- A set of useful **action plans** to support a focus on key considerations (Annex 2)
- A **Business Continuity Management Framework** (Annex 3)

3.7 The silver level response may require the formation of an **Incident Management Group**. This should where possible, be supported via a shared MS Teams group chat with relevant response leads.

3.8 Out of hours arrangements

The process above will be adopted out of hours, but the following on-call arrangements:
will be in place to ensure 24/7/365 cover:

- **Bronze level response:** Appropriate out of hours on call arrangements for student support, estates matters, crisis communications, IT services; and support for specialist academic areas will be in place and shared with the Campus Safety Team (who operate in and out of hours on a permanent basis).

- **Silver level response:** Will be the Chief Operating Officer or a named on-call delegate of the Chief Operating Officer (drawn from their direct reports) to provide a co-ordinating role for incident and business continuity planning out of hours. Out of hours, this delegate will be required to execute their responsibilities as if during working hours. While there is no absolute requirement to attend campus, they should be able to perform their responsibilities via telephone when called and be able to access MS Teams within no more than one hour (if required).

- **Gold level response:** No additional out of hours arrangements beyond formal delegation of responsibilities from the Vice Chancellor to Deputy Vice Chancellor and Provost in the absence of the Vice Chancellor. This ensures no period without the authority of the Vice Chancellor in place. The Chief Operating Officer (or acting Chief Operating Officer) should be aware of any out of hours incident by inclusion in the established MS Teams chat for the incident.

3.9 **On-call arrangements:** Full details of bronze and silver level response on-call arrangements for school, faculty and professional services areas will be in place and maintained as outlined in the responsibilities section of this policy. This will include an on-call silver level response rota and full contact details. This will be supported by the role of Incident and Business Continuity Manager.

3.10 The lead role of the Directorate of Estate and Campus Service and Campus Safety Team

Most (but not all) rapid onset incidents leading to the risk of an incident are reported to the Campus Safety Team (in and out of hours). The Campus Safety Team constitutes a bronze level response and this includes engagement and collaboration with a range of other bronze level arrangements (in and out of hours). The previous arrangements for the Directorate of Estate and Campus Service and the Campus Safety Team to provide a silver level response out of hours for the entire university is now replaced by the above arrangements. The Directorate of Estate and Campus Service will continue to make appropriate out of hours arrangements to provide a bronze level response for both estate-related (e.g., on call emergency trades) and security/safety-related matters.

3.11 A possible lead role for other Faculties/Directorates

When there is a specific incident that is not most appropriately reported to the Campus Safety Team, it should be reported/directed to the relevant bronze level response. This might include issues relating to failure of some business processes (e.g., IT-related services), some off-campus incidents (e.g., major travel disruption affecting students) or the need for urgent requests for responses from The Press (e.g., in response to a press story providing reputational risk).

Part C: BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

4.1 An implicit consideration of incident management is the potential for an incident to disrupt the operation of key functions and critical activities. The policy aims to develop a more explicit institutional approach to considering a range of potential impacts to business continuity. Existing approaches have rightly focused on impacts relating to our estate. This policy aims to further develop this approach and follow an established business continuity management framework to support incident management and preparedness of disruption to:

PREMISES: the physical estate and its services
PEOPLE: staff, students, visitors, and other people on and off campus or and anywhere;
PROCESSES: including our digital services and underpinning business infrastructures
PROVIDERS: our suppliers and partners on who we rely
PROFILE: our brand and our reputation

4.2 The policy aims to better support incident management using a business continuity management framework (Annex 3) to support management decisions in the event of a specific incident and to also develop a number of scenarios against which specific business continuity plans will be developed. The use of a business continuity management framework in this way aims to support the following key considerations in securing business continuity:

1. **Identification** of key assets and functions at risk in an incident (premises, people, processes, partners and profile) over a range of timescales;
2. **Assessment** of the impacts on these assets and/or functions and establishment of tolerable periods of disruption over a range of timescales;
3. **Dynamic** risk assessment to support initial impact assessments and impact of measures;
4. **Establishment** of key priorities to sustain levels of business continuity informed by (2 and 3);
5. **Documentation** of critical decisions
6. **Deployment** of appropriate resources
7. **Delivery** of measures to deliver business continuity and impact assessment of them.

4.3 Annex 3 provides a guidance framework which can be used to inform decision making in response to a particular incident and as the basis of the further development of business continuity plans for use during an incident. The policy establishes the following business continuity plans as a priority for further development:

1. Managing the impact of loss of IT service due to a cyber or ransomware attack
2. Managing the impact of incidents preventing use of student residences
3. Managing the impact of (and preventing) terrorist attack

Part D: IMPLEMENTATION, MONITORING, GOVERNANCE and PUBLICATION

5.1 Incident and Business Continuity Manager

This policy will be monitored and reviewed by the Chief Operating Officer, supported by an Incident and Business Continuity Manager who will report to the Head of Health and Safety within the Chief Operating Officers Office. The main duties and responsibilities of the Incident and Business Continuity Manager will be to:

- Work with senior leads and key stakeholders across the University to support them develop, review and continually improve the University's incident management and business continuity policy, protocols and plans to ensure these are aligned with institutional requirements and best practice, and are fit for purpose.
- Work with senior leads and key stakeholders across the University to implement and manage a comprehensive approach to incident management and business continuity.
- Support Faculties and Directorates to develop and regularly review their local incident management protocols and plans to ensure alignment to the University's Policy and framework.
- Work with senior leads to develop, co-ordinate, review, evolve and test the University's structured protocol/plan(s) with scenario-based exercises.
- Co-ordinate and deliver a bespoke training programme for specific command levels to assist them to understand their roles in the context of incident management and business continuity and to ensure practice responding to incidents.
- Develop and maintain the University's Incident Management and Business Continuity intranet site, materials and infrastructure, anticipating and acting on changing requirements to promote awareness to the University's community.
- Continually improve the approach to incident management and business continuity through working with senior leads on the review of all lessons learnt post-incident.
- Work closely with and support the Incident and Business Continuity Management Group as a key member and drive forward the implementation of the University policy and framework for incident management and business continuity.
- Engage on behalf of the University in the various communities of practice of business continuity management professionals, both within and beyond the HE sector, to ensure the University remains aligned with recognised best practice, such as Business Continuity Institute guidance and ISO BS Business Continuity standards.

5.2 Incident and Business Continuity Management Group

An Incident and Business Continuity Management Group (IBCMG) will be formed and be chaired by the Chief Operating Officer. The terms of reference of this group will be to:

- Agree an annual programme of work to review incident and business continuity management;
- Develop a priority set of business continuity plans to support the management of incidents relating to our IT services, student residences and terrorist attack;
- Review local area incident management protocol(s)/plan(s);
- To review and act on lessons learnt from incident and business continuity management which takes place in response to specific incidents;
- To horizon scan for new and emerging risk(s) and monitor relevant legislation.
- To review its own terms of reference and constitution annually.

IBCMG will be chaired by the Chief Operating Officer. Members of the group will include: Deputy Director of Estate and Campus Service; Head of Student Wellbeing; Head of Campus Safety Team; Cyber Security Manager; Head of Health and Safety; and the Head of Faculty Operations for the Faculty of Medicine and Health Sciences. The Incident and Business Continuity Manager will be secretary to the committee, which will meet bi-monthly.

5.3 This Policy and its supporting documents can be found on the **Policy Zone** and **Incident Management and Business Continuity intranet pages** on Keele University Internet and Staff Intranet.

Part E: POLICY EFFECTIVENESS and REVIEW

6.1 The Chief Operating Officer shall ensure that a formal post-incident review is undertaken within one month of any incident. This will be overseen by the Incident and Business Continuity Management Group. The review should include:

- An overview of the incident and how it was resolved;
- Agreed timelines for implementation of any improvements and changes;
- Debriefing and lessons learnt in responding to the incident.

6.2 Testing the agility in our management response

At least two incident management and business continuity exercises should be carried out each year with the scope and objectives agreed in advance. This will include the use of a realistic scenario to test the robustness of all aspects of the policy, but with a particular focus on:

- Robustness of the approach to use and escalation through the command structure
- The use of frameworks for risk assessment, command responses and business continuity
- The usefulness of any established bronze level protocols
- The usefulness of any established business continuity plans

Part F: TRAINING and INFORMATION

7.1 In addition to scenario exercises, appropriate training, with refreshers biennial, should be provided to members of staff who are involved in the silver and gold level response structure. An incident management and business continuity management intranet site will be established to place this policy and provide a set of more general information to communicate arrangements.

ANNEX 1: HOW TO MAKE A DYNAMIC RISK ASSESSMENT

What is Dynamic Risk Assessment (DRA)?

A DRA is a process of quickly identifying the potential likelihood and impact of an incident on business continuity. It is used when risks change quickly due to rapidly changing conditions which are common during incidents.

What is the difference between a risk assessment and a DRA?

A standard risk assessment is conducted on relatively static issues to determine risks and proactively come up with measures. It is commonly documented and forms the basis of established risk registers for a wide range of uses. A DRA on the other hand is more spontaneous approach to risk assessment, especially in high-risk situations, such as in declared major incidents, where it is conducted on the spot when there is a sudden change in the situation and risks need to be immediately identified, controlled and mitigated. The approach to DRA requires a focus on the development of competency and agility in real-time risk assessment and mitigation.

Using DRA to define an incident and use in business continuity

A DRA can be conducted using the matrix below to derive an initial severity score of the impact of the incident to business continuity, and to guide the levels of command response likely to be required. The overall assessment (low, medium or high risk) considers both likelihood and severity of impact of incidents to business continuity (and also the impact of mitigations to manage these risks).

Severity score						
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Likelihood score	Rare (1)	Low	Low	Low	Low	Moderate
	Unlikely (2)	Low	Low	Moderate	Moderate	Moderate
	Possible (3)	Low	Moderate	Moderate	Moderate	High
	Likely (4)	Low	Moderate	Moderate	High	High
	Certain (5)	Moderate	Moderate	High	High	High

High: Rating 15 or more GOLD, SILVER & BRONZE RESPONSE	Moderate: Rating 9-12 SILVER & BRONZE RESPONSE	Low: Rating 1-8 BRONZE RESONSE
Immediate action is required to control and/or lower the level of risk of business continuity to large parts or all the university's key functions. All three levels of command response.	Urgent action to control and/or lower the level of risk to business continuity to all or some parts of the university's key functions. Bronze and Silver levels of command response engaged.	Usually, no further action will be required beyond a bronze level of response, except for monitoring to ensure the risk does not change.

ANNEX 2: SILVER and GOLD LEVEL ACTION PLAN TEMPLATES

These action plan templates present a method to aid on focussing on priority issues. These actions focus on essential information and instructions required to perform a specific role, task or function whether in or out of hours. They are not intended to be exhaustive, as there may be other duties required which are not listed.

Silver level response key actions
Get a clear briefing from the bronze level response
Accept or decline request for a silver level response
Bronze to confirm on-going response with silver
Decide whether or not to establish an Incident Management Group
Establish a clear approach to logging issues and decisions
Establish an MS Teams Chat to support incident
Carry out a dynamic risk assessment
Use the business continuity management framework to prioritise actions
Carry out a dynamic risk assessment to assess impact of priority actions
Consider requirement to engage all areas in a response including external agencies
Approve approach to internal and external communications
Establish any major resourcing requirements and provide permission appropriate to your level of delegation
Consider well-being of those handling the incident
Brief gold level response, as and when appropriate
Consider need to request gold level response
Support and co-ordinate bronze level responses, do not replace this level of response

Gold level response key actions
Get a clear briefing from the silver level response
Accept or decline request for a silver level response
Consider any specific major reputational, compliance or legal impacts
Decide on the need for a gold-level incident response group
Silver to confirm on-going approach and the bronze level response
Establish any major resourcing requirements and provide permission
Approve approach to internal and external communications
Consider any immediate but non-emergency external notifications e.g. ICO, HSE, OFS, Police, insurers, legal advisors
Support silver level response, do not replace this level of response

ANNEX 3: KEY STEPS for the BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

What is the Business Continuity Management Framework?

The Business Continuity Management Framework (BCMF) is a structured way of understanding the impacts of an incident and how to prioritise business continuity measures to reduce levels of risk and disruption, against a determined level of tolerable disruption (including the period of disruption). It can be used to inform business continuity planning during an incident and form the basis for the development of business continuity plans in advance to support decision making during incident management.

Below are 7 key steps of the BCMF. The specific impacts of an incident will differ depending upon the nature of it as will the consequent management responses. The framework highlights some of the key considerations in business continuity planning, by considering, assessing, prioritising and delivering management responses to manage impact on our premises, people, processes, partners and profile.

This framework will inform the development of business continuity plans, with a priority to managing the impact of:

- Loss of IT service due to a cyber or ransomware attack
- Managing the impact of incidents preventing use of student residences
- Managing the impact of (and preventing) terrorist attack

Seven key steps:

1. Identify the key functions or asset at risk

This should consider the impact on premises, people, processes, providers and profile and the impact over differing periods of time relevant to the incident e.g. immediate impacts v. those which might develop over time.

2. Evaluate the potential impact of disruptions.

This should consider how long a disruption can last before a level of disruption is un-acceptable. A maximum length of time that a disruption can be managed is referred to as the Maximum Tolerable Period of Disruption (MTPD).

3. Undertake a dynamic risk assessment (DRA)

This should focus the critical activities and supporting resources identified. Conducting a risk assessment will look at the likelihood and severity of a variety of risks that could cause a business interruption. By assessing these, risk reduction activities can be prioritised.

4. Establish the objective(s).

This aims to establish a realistic assessment of when functions or assets may or need to be restored and a priority to their restoration (via a. Timelines for interim (temporary) solutions. b. Timelines for permanent solutions). This is often referred to as the Recovery Time Objective (RTO).

5. Document the critical activities that are required to deliver the key functions.

This aims to provide clear communication of decisions agreed and as a record for review.

6. Quantify the resources required to provide a determined level of business continuity.

This can include resources needed to redress impacts across the 5 potential areas impacted during an incident. Some possible considerations, incident-dependent, are set out below.

Premises:

What locations do the critical activities operate from?

What alternative premises are there?

What plant, machinery, assets and other facilities that are essential to carry out the critical activities?

People:

What is the ideal number of staff you require to carry out the critical activities?

What is the minimum staffing level with which could provide some sort of activity?

What skills/level of expertise is required to undertake these critical activities?

Processes:

What IT is essential to carry out the critical activities?

What systems and means of voice and data communication are required to carry out the critical activities?

What information is essential to carry out the critical activities?

How is this information stored?

Providers:

Who are priority suppliers/partners that are depended on to undertake the critical activities?

Are key services tendered out to another organisation, to whom and for what?

Are there any reciprocal arrangements with other organisations?

Profile:

How could reputational damage be reduced?

How would information to staff, students and others in an emergency be provided?

Are there systems to log decisions, actions and costs, in the event of an incident?

How could vulnerable groups be contacted/accommodated in the event of an incident?

7. Determine business continuity solutions/arrangements

This step is about identifying the action(s) to take to maintain the critical activities that underpin the delivery of the key functions, informed by the above steps and risk assessment. Having previously determined the RTO for each critical activity, there should be a strategy for meeting it. This involves taking appropriate action to mitigate the loss of the resources that has been identified in Step 5. The below provides some of the tactics to establish in advance to support business continuity or deploy in the management of an incident.

Premises:

Relocation of staff, students and others to other accommodation

Displacement of staff, students and others performing less urgent activities, processes with staff, students and others performing a higher priority activity

Remote working – this can be working from home or working from other locations.

Use premises provided by other organisations, including those provided by third-party specialists

Alternative sources of plant, machinery, assets and other equipment.

People:

Inventory of staff skills not utilised within their existing roles – to enable redeployment.

Process mapping and documentation – to allow staff to undertake roles with which they are unfamiliar

Multi-skill training of each individual

Cross-training of skills across a number of individuals

Succession planning and deputization arrangements

Use third party support, backed by contractual agreements.

Geographical separation of individuals or groups with core

Processes:

Maintaining the same technology at different locations that will not be affected by the same business disruption.

Holding older equipment as emergency replacement or spares.

Ensure data is back-up and it is kept off site.

Essential documentation is stored securely (e.g., fireproof safe).

Copies of essential documentation are kept elsewhere.

Providers:

Storage of additional supplies at another location.

Dual or multi-sourcing of materials.

Identification of alternative suppliers.

Encouraging or requiring suppliers/partners to have a validated business continuity capability.

Significant penalty clauses on supply contracts.

Mechanisms in place to provide information to stakeholders.

Arrangement to ensure vulnerable groups are accommodated.

Profile:

Communication strategy/plan/procedures in place.

Stakeholder liaison (regulator, clients, Unions) are carried out.

Media liaison considered.

Public information/advice provided to the University community.

Notification of at-risk groups with alternative arrangements.

DOCUMENT CONTROL INFORMATION

Document Name	Incident & Business Continuity Management Policy
Owner	Chief Operating Officer
Version Number	1.0
Equality Analysis Form Submission Date	Not undertaken
Approval Date	06 July 2023
Approved By	Council
Date of Commencement	01 August 2023
Date of Last Review	[Day/month/year]
Date for Next Review	01 July 2026
Related University Policy Documents	[List all applicable]
For Office Use – Keywords for search function	