Incident Management and Business Continuity Policy

Document Type	Policy
Document owner	Ayisha Govindasamy (Head of Governance)
Approved by	Executive Team
Approval date	09 May 2024
Last review date	May 2024
Next review date	May 2025
Version	1.0
Amendments	N/A
Related Policies & Procedures	Risk Management Policy Incident Management Procedures Recovery Procedures Reportable Event Procedure

1. SCOPE

1.1 This policy will operate across all areas of the LSHTM, including the MRC/UVRI & LSHTM Uganda Research Unit (MRCU) and the MRC Unit The Gambia at LSHTM (MRCG).[1]

1.2 Across the London, MRCU and MRCG there will be differences in the application of this policy to accommodate differences in context and operations, however such variations will:

1.2.1 prioritise the safety and welfare of all interested parties,

1.2.2 allow the LSHTM to uphold its legal obligations (including those with regards to the Units), and

1.2.3 support the shared strategic aims of the Units and the LSHTM.

1.3 Two distinct yet interlinked areas are covered by this policy:

1.3.1 **Incident Management** is focused on the immediate response to an incident and its on-going governance, to minimise its impact on the welfare and safety of people, and to contain the impact on the LSHTM's operations and strategic objectives. This is addressed by the Incident Management Procedures, and also by Incident Recovery Procedures (recovery of IT infrastructure, and physical resources) at local levels.

1.3.2 **Business Continuity** is focused on ensuring critical activities can be carried out in the event of significant disruption to LSHTM's systems, services, structures and infrastructure. This is addressed by Business Continuity plans at organisational and local levels.

1.4 Certain services, particularly those that are owners of physical and digital assets, also have Incident Recovery Procedures that can be activated in response to an incident affecting that area.

[1] For the remainder of this document, any reference to The LSHTM includes MRCU and MRCG, unless it is clearly specified otherwise.

1.5 In the event of an incident interested parties may include: LSHTM governing body (Council), staff members, current and prospective students, external suppliers, services and contractors, funding bodies, regulatory bodies, visitors, neighbouring organisations and external individuals or organisations collaborating with individuals of groups within the LSHTM.

1.6 The LSHTM's Incident Management and Business Continuity procedures are designed to support a response to different types of incident, which can be defined as:

1.6.1 **Minor Incident** – an incident that has negligible impact on, or may briefly disrupt the normal course of, business operations, and which will be dealt with by routine operational management.

1.6.2 **Serious incident** – an incident that may cause serious disruption to business operations, and/or may involve major injury or serious illness. It may require the initiation of Incident Response Plans in the Incident Management Procedure and the implementation of local Business Continuity plans.

1.6.3 **Major incident** – an incident which significantly affects a large proportion of the LSHTM's community or operations, may pose a serious threat to life, and where normal management arrangements are insufficient. A major incident would invoke the relevant Incident Response Plans within the Incident Management Procedure, and the Incident Management Team, and would usually require the implementation of Recovery and Business Continuity plans.

2. PURPOSE AND AIMS

2.1 The purpose of Incident Management and Business Continuity is to ensure the resilience of LSHTM in the event of significant disruption, enabling the School to continue to deliver on its strategic objectives and overall mission to improve health and health equity in the UK and worldwide.

2.2 To ensure a clear, consistent and coordinated approach to Incident Management and Business Continuity across the LSHTM, facilitating appropriate decision-making, escalation and information sharing that will ensure the safety and welfare of all interested parties, ensure the continued delivery of critical operations, and allow a return to business as usual as quickly as possible.

3. OBJECTIVES

3.1 To identify all critical activities across the LSHTM.

3.2 To proactively consider major risks to these operations that may result in significant disruption.

3.3 To identify mitigating actions that can be implemented proactively to improve resilience.

3.4 To identify appropriate contingency plans to deliver critical activities in the event of serious disruption.

3.5 To establish structures to plan for and respond to incidents, including robust and relevant Incident Management, Incident Recovery and Business Continuity plans, both at organizational and service levels (as appropriate), as well as the identification of appropriate communication channels.

3.6 To provide guidance, advice and training where necessary for staff members.

3.7 To ensure all relevant documentation is subject to regular testing, review and updating, and is readily available to appropriate staff in the event of an incident.

4. GOVERNANCE

4.1 Incident Management and Business Continuity fall under the remit of the LSHTM's internal Risk Management Group in line with their Terms of Reference. Identification of risks and threats is outlined separately in the Risk Management Policy.

4.2 Policy approval and overall accountability for Incident Management and Business Continuity reside with the Executive Team in line with their Terms of Reference.

4.3 At Council level, Incident Management and Business Continuity are under the remit of the Audit and Risk Committee.

4.4 The Executive Team owner for Incident Management and Business Continuity is the Chief Operating Officer.

5. ROLES AND RESPONSIBILITIES

Acronyms:

COO	Chief Operating Officer
FOO	Faculty Operating Officer
HoS	Head/s of Service
IMP	Incident Management Procedures
IMT	Incident Management Team
LBCT	Local Business Continuity Team (service level)
OCDO	On Call Duty Officer

5.1 Overall accountability for Incident Management and Business Continuity lies with the LSHTM Director, however, responsibility for implementation is delegated to the Executive Team owner and the administrative owner. In the line with the LSHTM Schedule of Delegation the Unit Director is accountable to the LSHTM Director for local implementation, supported by the Unit COO.

5.2 As the Executive Team owner of Incident Management and Business Continuity, the LSHTM COO will:

5.2.1 Chair the IMT or appoint a delegate to do so.

5.2.2 Activate the LSHTM Business Continuity plan where disruption to business operations has occurred or is likely to occur.

5.2.3 Be responsible for communication and engagement regarding Incident

Management and Business Continuity with the wider LSHTM community.

5.2.4 Promote the embedding of robust Incident Management and Business Continuity practices across the organisation.

5.2.5 Ensure timely communication with staff at the Units where required for Incident Management. The Incident Management Procedures contain trigger points for communication which should be reflected in local plans.

5.3 As the administrative owner of Incident Management and Business Continuity, the Head of Governance, will:

5.3.1 Initiate and monitor the annual testing and review cycle for all Incident Management and Business Continuity documentation, and ensure owners update their documents.

5.3.2 Be responsible for the management of the repository where all Incident Management and Business Continuity documentation is stored.

5.3.3 Bring Incident Management and Business Continuity matters to the Risk Management Group.

5.3.4 Report on Incident Management and Business Continuity at the LSHTM Audit and Risk Committee.

5.3.5 Make timely amendments to this policy, the Incident Management Procedures and the LSHTM Business Continuity plan following review, ensuring version control, and submit the amended documentation to the Risk Management Group for review.

5.3.6 Following an incident, support the IMT to ensure adherence to policy and procedures throughout the incident response.

5.3.7 Ensure that a 'lessons learned' debrief takes place following any incident where the IMT has been assembled, and receive post-incident reports to sign off and bring to the Risk Management Group.

5.4 The IMT will:

5.4.1 Take responsibility for, and monitor, the implementation of the Incident Management Procedures and Business Continuity measures in the event of a disruptive incident, and support the Chair of the IMT as required.

5.4.2 Take decisions in the event of an incident and inform the Executive Team, as well as informing other relevant key stakeholders, or escalate to the Executive Team where appropriate.

5.4.3 Inform the Administrative Owner of any changes or developments they are aware of which will require edits to the Incident Management Procedures, and inform the Head of Security of the necessity to change or confirm any relevant contact details.

5.5 HoS and FOOs will:

5.5.1 Be responsible for the identification of critical activities within their area/faculty and the consideration of major risks to these.

5.5.2 Identify appropriate mitigating actions and ensure their implementation.

5.5.3 Identify appropriate contingency plans and be responsible for the completion, regular review and updating of the Business Impact Analysis and Business Continuity plan for their service/faculty, as well as any Incident Management/Recovery Procedures that they own.

5.5.4 Activate the Incident Management/Recovery Procedures that they own and/or Business Continuity plan in response to an event in the service/faculty that requires a response.

5.5.5 Be responsible for the implementation of Incident Management/Recovery and Business Continuity measures in their service/faculty.

5.5.6 Engage with training and testing exercises, ensure they are informed about Incident Management and Business Continuity procedures as applicable, and cascade this information as appropriate to staff and others within their remit.

5.6 The MRCG and MRCU COOs will:

5.6.1 Be responsible for the identification of critical activities within the Unit and the consideration of major risks to these.

5.6.2 Identify appropriate mitigation actions and ensure their implementation.

5.6.3 Identify appropriate contingency plans and be responsible for the completion, regular review and updating of the Business Impact Analysis and Business Continuity plan for the Unit, as well as any Incident Management/Recovery Procedures that they own.

5.6.4 Activate the Incident Management/Recovery Procedures that they own and/or Business Continuity plan in response to an event at the Unit that requires an incident response.

5.6.5 Be responsible for the implementation of Incident Management/Recovery and Business Continuity measures at the Unit.

5.6.6 Engage with training and testing exercises, ensure they are informed about Incident Management and Business Continuity procedures as applicable, and cascade this information as appropriate to staff and others within their remit.

5.6.7 Be responsible for appropriate and timely communication with LSHTM London regarding any incidents that are occurring or have occurred at the Unit, including notifying the London COO and Director, and other relevant staff (such as the Director of ITS for cyber events). The LSHTM Incident Management Procedures contain trigger points for communication which should be reflected in local plans.

5.7 LBCTs are responsible for supporting their HoS/FOO/Unit COO with the development, maintenance and implementation of Incident Response and Business Continuity measures within their area

5.8 ODCO is responsible for:

5.8.1 Being contactable when on call, categorizing an incident, activating an incident

response plan from the IMP when applicable, and assembling the appropriate team for the incident response.

5.9 The Head of Security will:

5.9.1 Ensure that relevant documentation in the emergency boxes (at reception of London sites) is kept up to date and accessible, sending regular reminders (not less than twice yearly) to document owners to review and update their documentation, maintaining a register of documents and their ownership and maintaining the physical and electronic repositories for this documentation.

5.9.2 To induct new OCDOs and oversee the management of the OCDO rota.

5.9.3 Keep the OCDO contact information and Key Contacts document up to date.

5.9.4 Take on a coordinating and supporting role before and during an incident, overseeing the Security team that manages access to the buildings, switchboard and supporting logistics.

5.9.5 Facilitate annual training and testing exercises, in liaison with the owner of the IMP and Business Continuity procedures

6. MONITORING, EXERCISING AND REVIEWING

6.1 Annual testing exercises will be carried out to ensure the Incident Management Procedures, local Incident Recovery Procedures and the Business Continuity plans are fit for purpose. Recommendations will be made for improvements to policies, procedures and templates as required. Additional testing may be carried out throughout the year subject to local schedules and standard operating procedures (e.g. within IT Services).

6.2 Testing exercises will include all document owners for Incident Management, Incident Recovery and Business Continuity as appropriate.

6.3 Following exercises, all documentation must be reviewed and updated by document owners. Relevant Health and Safety, IT or other service owned documentation may also be updated at this point to ensure consistency across policies and procedures.

6.4 Document owners are responsible for ensuring clear version control, ensuring outdated documents are withdrawn from circulation and that all relevant parties are aware of changes made.

6.5 This policy will be subject to review by the IMT and will be updated by the Administrative Owner. Updates will be submitted to the Risk Management Group by the Administrative Owner and onward to Executive Team.

6.6 Following an incident, there will be a ‘lessons learned’ review of relevant Business Continuity plans, the incident management procedure and this policy as applicable. This will be carried out in the same way as detailed in 6.2 to 6.5. Following a major incident, a report will be completed following the guidance in the IMP. A report may be completed following a serious incident, at the discretion of the response team lead. Reports will be submitted to the Risk Management Group by the Administrative Owner.

6.7 Lessons learned reports compiled at the MRC Units should also be submitted to the

Risk Management Group by the relevant Unit COO or their delegated representative.

7. POLICY SIGN OFF AND COMMUNICATION

7.1 This policy is to be signed off by the Executive Team at the LSHTM. Executive Team will also approve any subsequent amendments to the policy and the updated version will be shared with Council and its sub-committees on request.

7.2 This policy will be available online with other LSHTM policies. All staff involved the IMT/LBCTs must read and understand the policy.