IT Disaster Recovery Policy

Document Type	Policy
Document owner	Graeme Cappi, Director of IT Services
Approved by	Management Board
Approval date	13 January 2021
Review date	January 2022
Version	1.0
Amendments	-
Related Policies & Procedures	LSHTM Service Catalogue IT Major Incident Plan

1. SCOPE

1.1 LSHTM Wide – all staff and students

1.1.1 Core IT Services Managed systems and services

1.1.2 Cloud based LSHTM Managed Services

2. PURPOSE AND OVERVIEW

2.1 This policy provides a framework to define the ongoing process of planning, developing and implementing IT Disaster Recovery management for the London School of Hygiene and Tropical Medicine.

2.2 It defines the current methods of management and mitigation of IT systems and services, including data on behalf of LSHTM.

2.3 It provides and overview of the system approach that should be taken in order to safeguard the critical technology and data managed by IT Services at LSHTM, and how that approach should be implemented.

3. POLICY

3.1 Introduction

This policy provides a framework to define the ongoing process of planning, developing and implementing IT Disaster Recovery management for the London School of Hygiene and Tropical Medicine.

It defines the current methods of management and mitigation of IT systems and services, including data on behalf of LSHTM.

A disaster is defined as a serious incident that cannot be managed within the scope of LSHTMs normal working operations

3.2 Requirement for the Policy

This policy provides an overview of the systematic approach that should be taken in order to safeguard the critical technology and data managed by IT Services at LSHTM, and how that approach should be implemented.

3.3 Definitions

Disaster Recovery Operations

- All activities and steps necessary to restore systems services that are affected by a disaster.
- All activities concerned with management and user communications related to the disaster.
- All activities concerned with the mitigation of the impact of an ongoing disaster incident.
- All activities concerned with the follow-up to an incident

Disaster Recovery Management

- Identify critical and secondary systems based on risk assessment.
- Establish baseline recovery time capabilities and objectives.
- Maintain and test DR capabilities on an ongoing basis.
- Identify gaps between current and required capabilities for system recovery.

3.4 IT Disaster Recovery Policy Objectives

DR Management

This policy exists to minimise the impact of any significant incidents on LSHTM systems and services, to recover from the unavailability of those systems to an acceptable level, and to define the controls to do so (i.e. response and recovery controls)

In order to be able to achieve this there are 3 main objectives:

- Establish Operational Control of the Disaster (the War Room)
- Communicate with relevant parties impacted by the disaster (the Comms Plan)
- Activate a specific recovery plan(s) relevant to the situation (Run Books)

The operational process for invoking DR, the criteria used to define it and the roles which are needed in order to progress each runbook for the restoration of service(s) is contained in the LSHTM Major Incident Plan (IT-MIP)

Disaster Recovery Planning

LSHTM IT Services shall conduct risk assessments and ensure scenarios, procedures and plans are developed and implemented for critical business systems to ensure timely resumption of essential services. These are known as Runbooks and should be made available to all technical IT that may need to be involved in service restoration (DR Teams) and will need to be regularly tested

and updated as necessary. Copies of the Runbooks, and the Major Incident Plan should also be kept securely off-site and available out of hours.

Where critical services are outsourced, IT Services shall ensure that suppliers agree to have similar suitable plans and contingencies in place to meet the criteria for critical systems.

The provision of enterprise IT infrastructure has to be a balance between affordability and availability, and it is therefore not possible to maintain fully redundant hardware in preparation for all or any potential disasters. LSHTM has two main data centres, located in each of the Keppel Street and Tavistock Place buildings. It has implemented cross data centre resilience, where either data centre has the capability to provide adequate operating services in case of the loss of a single data centre. Disaster recovery is incorporated into the architecture of new systems that are deemed critical by the business, or so defined by their Service Level Agreement (SLA)

The recovery of a service is governed by the stated, agreed Recovery Time Objective (RTO) for each service, and the level of criticality of each system. A service is a collection of systems and devices that collectively support a business process. For all core LSHTM IT Services the details for this are provided by their Service Catalogue entry (LSHTM Service Catalogue - Home (sharepoint.com)).

The recoverability of a service is governed by the capabilities of the underlying systems in terms of resilience and redundancy, and the time for recovery of the systems in the event that recovery is required.

Gold	A Gold level service is any critical system necessary to support the core operational delivery requirements of LSHTM. These services should be defined by the Corporate Information Systems Board, and supporting systems identified through further analysis.	All Gold systems are fully resilient and redundant across dual-data centres. The design recovery time objectives (RTO) for Tier 1 systems are a maximum of 24 hours. The minimum essential services for all critical systems are identified and documented. Significant projects and changes associated with these services must have documented and tested contingency plans- e.g. back out plans, contingency services, extended change outage windows.

Silver	A Silver level service is any other non-critical system operated or managed by IT Services as a production system for University operations.	Tier 2 systems have a designed maximum recovery time objective (RTO) of 72 hours, and all minimum essential services are identified to ensure efficient recovery. Minimally, all Tier 2 data shall be recoverable from remote offline backup storage media, and where necessary and feasible, full systems shall be backed up. Significant projects and changes associated with these services must have documented contingency plans.
Bronze	A Bronze service is one which the Service Owner defines as needing no resilience or failover.	These are services which are able to tolerate extended downtime of up to two weeks with no significant impact on operations. They should be designed with manual workarounds where necessary via the provision of short term or temporary facilities to accommodate user requirements.

The infrastructure and systems associated with each service should be identified and clearly defined. A Service Owner for service should be identified and recorded and the details of this responsibility documented. This information is held in the LSHTM IT Service Catalogue.

Standard appropriate maintenance contracts for critical components should be in place. In case of component or hardware replacement, vendor contacts are identified and easily accessible.

For each service, the following data shall be maintained by the Technical Service Manager:

- Key service data: Service Owner, Technical Service Manager, platform details, backup mechanism, recovery mechanism, system tier ranking.
- Key operational procedures for startup, shutdown and recovery of all systems associated with the service.
- Key contacts for suppliers, SLA details or maintenance contract details where relevant, and incident invocation and escalation procedures for the supplier.
- Test schedule for system components, and full service test schedule. The following general data shall also be maintained:
    - Contact lists for University Senior Management and IT Services committees.
    - Contacts for key University services - Buildings and Services, Communications Office, Corporate Secretary's office.

The Head of Information Security shall be responsible for the collection, management and distribution of the DR Policy and Procedures.
Service Managers and delegated systems administrators shall prepare and maintain procedures and plans as required under this policy.

Disaster Recovery Plan Testing

Where possible, disaster recovery documents, specifically this policy, the procedures and plans, shall be tested and updated to ensure that they are up to date and effective, especially following significant system changes.

System level testing, including the physical hardware is tested on a regular basis, to ensure that it operates as required and agreed with the service owner. Responsibility is assigned to Service Managers as identified by procedure to ensure that this is carried out in a correct manner, and should be reflected in the Service Catalogue entry.

Operational procedures shall be reviewed by Service Managers after significant or major changes to underlying systems, and testing of services shall coincide with planned major upgrades.

Regime

ITS will perform the following DR testing (which is in addition to the testing requirements set out by each Service Owner and Manager for their individual service as noted above):

Twice yearly full DR scenario testing. The scenario will be defined and agreed by the ITDR Governance Forum, and should also be aligned to any LSHTM Major Incident Team testing.

Annual scenario desktop based DR exercise, defined and agreed by the ITS Senior Management Team – designed to test the Major Incident Response Plan.

3.5 Disaster Recovery Process

Disaster recovery management is incorporated in IT Services processes and structure

The activities for disaster recovery management shall be coordinated by representatives from different parts of IT Services with relevant roles and job functions. This co-ordination involves the collaboration of several separate teams and is noted in detail in the IT Major Incident plan referenced above in the DR Management section.