Maynooth University
IT Services

Maynooth University
IT Services Disaster Recovery (DR) Policy

Version 1.3

Maynooth University
IT Services
Maynooth, Co. Kildare, Ireland.

Seirbhísí TF
Ollscoil Mhá Nuad
Má Nuad, Co. Chill Dara, Éire

T +353 1 708 3388 **E** servicedesk@mu.ie **W** maynoothuniversity.ie

Revision Record

Author / Policy Owner:	IT Services: Head of IT Operations	
Version 1.0	Creation	6 January 2020
Version 1.1	Feedback from HEAnet	9 June 2020
Version 1.2	Feedback and text incorporated in MU Policy Template	15 June 2020
Version 1.2	Text approved following internal review	26 June 2020
Version 1.3	Updated following HEAnet ICT Security Services review and review by IT Services Management.	15 December 2022
Next Review Date:		Q2 2026

Table of Contents

Section One

1. Policy Statement

This policy provides a framework for the ongoing process of planning, developing, and implementing disaster recovery management for services provided by IT Services only.

For the purposes of this policy, a disaster is a serious incident that cannot be managed within the scope of IT Services' normal working operations.

2. Policy Scope

This policy applies to all services and systems hosted or managed by IT Services unless specifically excluded by a service level agreement. This policy will provide for:

- Disaster Recovery Plans created under this policy
- Risk Assessments and Business Impact Analyses conducted in support of this policy
- Disaster Recovery exercises and testing to be conducted in support of this policy or an associated plan. The frequency and outcome of tests and exercises is stored as part of the DR plan documentation set.
- The management of any activities concerned with the mitigation of the impact of an ongoing disaster incident.
- Communications in relation to any disaster recovery activity encompassed by this policy.

For the purposes of this policy, the term Disaster Recovery Plan may refer to a collection of any or all the above-mentioned documents.

3. The Purpose of the IT Services Disaster Recovery Policy

The purpose of this policy is to provide a process of planning and preparation which will enable the restoration of mission critical IT systems and services to a running state after an outage.

This management approach is implemented to minimise the impact of major incidents on ICT services and to expedite recovery of systems and services to an acceptable level through a combination of responsive and recovery controls.

4. Policy Principles

4.1. Disaster Recovery Planning

A disaster recovery plan can be defined as the on-going process of planning developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of systems and services in the event of an unscheduled or unwanted interruption.

The Disaster Recovery Plan must be based on:

- A review of all services, to be reviewed annually and updated accordingly.
- Conducting risk assessments
- Conducting business impact analyses to identify mission critical functions and to determine their relationship to ICT systems and services

- Maintaining and testing Disaster Recovery objectives on an ongoing basis
- Provide for training on the Disaster Recovery Plan

These plans shall be made available in a convenient form for use by IT Services and shall be available to IT Services staff and periodically reviewed and updated. All documents will be available inside the IT Services Team on the IT Disaster Recovery channel.

4.2. Objectives of the Disaster Recovery Plan

The objectives of the Disaster Recovery Plan should include the following
- Establish operational control of the disaster
- Communicate with relevant parties impacted by the disaster
- Activate a specific recovery plan in relation to the disaster

4.3. Testing of the Disaster Recovery Plan

The Disaster Recovery Plan shall include a testing schedule to ensure:
- Baseline recovery capabilities and objectives can be met by the process.
- Preparedness: All IT Services staff relevant to a disaster recovery operation are familiar with process
- Established communication processes around disaster recovery are robust and fit for purpose

Records of tests carried out and lessons learned therefrom shall be retained.

4.4. Review of Disaster Recovery Plan

The Disaster Recovery Plan shall be reviewed after each invocation and updated accordingly in order that:
- Any gaps between current and required capabilities for service recovery can be identified and acted upon
- Any lessons learned from the test(s) shall be documented. If action is required, this should be reflected in an update of the Disaster Recovery Plan.

The Disaster Recovery Plan shall be reviewed at least once every 12 months if it has not been invoked in an intervening period.

4.5. Service Design in the Context Disaster Recovery

It is neither economical nor practical to maintain fully redundant equipment and services in preparation for all potential disasters.

IT Services has in the main implemented cross data centre resilience, where a 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 mission critical by the business. 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 (referred to as Level).

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

Where services are provided by 3rd parties, IT Services shall ensure that there is a contract and/or service agreement in place where it is agreed that similarly suitable plans and contingencies exist to meet the level of operation required for the services. (See Section 7 for DR levels).

4.6. Invoking the Disaster Recovery Plan

The disaster recovery plan is invoked when

- A member of the IT Services management team requests the commencement of disaster recovery activities according to the IT Services Disaster Recovery Plan.
- If a mission critical level 1 service sustains a service outage which has lasted 24 hours or is determined as likely to do so. Disaster recovery levels are detailed in Section 7 and outlined below.

Disaster Recovery Level	Name	Recovery Time Objective (RTO)
Level 0 - Mission Critical	MC	< 24 hours
A mission critical service requires continuous availability. Breaks in these services are intolerable and immediately cause damage to MU.		
Level 1 - Business Critical	L1	24 hours (next day)
A business-critical level 1 service requires continuous availability, though short breaks in service are not catastrophic. Availability required for effective business operation.		
Level 2 – Business Operational	L2	Within 48 hours
Contributing to efficient business operation but out of direct line of service to customer. Business operational services contribute to the effective running of the company but are out of the direct line of service to customers.		
Level-3 – Administrative Services	L3	Within 3 days
Services on the level of office productivity tools, required for business to operate. Failures are undesirable but do not affect customers and can be tolerated a little more. Cannot justify extreme additional expenses for higher availability		

4.7. Communicating During a Disaster Recovery Operation

In the event of a disaster recovery operation taking place, communications between IT Services and the University shall be carried out according to *the IT Services Major Incident and Communications Plan*. This provides for:

- **Major Incident Response Team** - the IT Services staff and any 3rd parties working to address the problem
- **Major Incident Manager** - an IT Services staff member leading the Major Incident Response Team.
- **Major Incident Coordinator** - an IT Services staff member responsible for communications and keeping all stakeholders informed of developments (especially UE).
- **Communications Team** – members of IT service working help the Major Incident Coordinator.

The form and method of the communications will be determined by the nature of the recovery operation and the communication methods available at the time, as provided for in the *IT Services Major Incident Communications Plan.*

4.8. 3rd Party Service Agreements

All new 3rd party services shall ensure that the contracts include provisions for disaster recovery operations. This should be validated through a service review process by the relevant IT Services manager and recorded in IT Services Disaster Recovery channel.

Disaster Recovery provisions shall be incorporated and validated into all existing services involving IT Services at their next review and also recorded in the IT Services Disaster Recovery channel.

Section Two

5. Roles and Responsibilities

5.1. Service Owners

The role of Service Owners is to actively engage with IT Services in the development of disaster recovery processes where they have resources hosted by IT Services.

- Promote and support the development of planning to avert potential disasters and risks to business continuity
- Support the development of enhanced IT resilience.

5.2. IT Services

The role of IT Services is to provide for and carry out disaster recovery planning by:

- Developing disaster recovery plans and reviewing them on an annual basis.
- Classifying systems and services according to levels of operational importance in conjunction with the Service Owner relevant to disaster recovery as indicated in Section 7.
- Maintaining an updated list of the owners and managers of all systems and services hosted and supported by IT Services.
- Conducting risk assessments on existing and planned systems or services
- Managing relationships with other departments and partners in the context of IT Disaster Recovery.
- Conducting disaster recovery tests.
- Reviewing and updating all disaster recovery plans and related processes on an annual basis.
- Ensuring that all IT Services staff and relevant partners receive the appropriate training on and awareness of this policy and any dependent plans and processes flowing from it.
- Communicating with University Executive, Service Owners, Heads of Departments, and the University Community as appropriate.
- Managing the testing of services in line with processes agreed with Service Owners and any relevant third parties.
- Defining the services to be included in the Disaster Recovery Plan and how that service is managed.
- Reviewing operational procedures after significant or major changes to underlying systems and services. This testing of the plan shall coincide with planned major upgrades.
- The Head of IT Operations shall ensure the collation, management and distribution of IT Services DR policy, plan and procedures. The relevant IT Service Managers and delegated systems administrators shall prepare and maintain procedures and plans as required under this policy.

5.3. Service Users

Some employees of Maynooth University manage or administer systems or services hosted by IT Services. The role of such Service Users is to

- Engage with IT Services in the development of disaster recovery planning for the services they manage or operate
- Facilitate the conducting of risk assessments and disaster recovery tests
- Co-operate with and assist IT Services in any disaster recovery activity.

6. Glossary of Terms

The following definitions are based on the ITIL Glossary of Terms at [ITIL® 4 Glossaries of Terms | Axelos]	
Active Monitoring	Monitoring of a configuration item or an IT service that uses automated regular checks to discover the current status.
Asset	Any resource or capability.
Business Continuity	The process of getting the entire business back up and running after a crisis.
Business Impact Analysis	Business impact analysis is the activity in business continuity management that identifies vital business functions and their dependencies. These dependencies may include suppliers, people, other business processes, IT services etc. Business impact analysis defines the recovery requirements for IT services. These requirements include recovery time objectives, recovery point objectives and minimum service level targets for each IT Service
Critical Success Factor (CSF)	Something that must happen if an IT service, process, plan, project or other activity is to succeed. Key performance indicators are used to measure the achievement of each critical success factor.
Disaster Recovery	The process of getting all systems and services running in line with their required level of operation after an outage e.g. hardware failure or power outage.
Mission Critical Service	A mission critical service requires continuous availability. Breaks in these services are intolerable and immediately cause damage to MU.
Passive Monitoring	Monitoring of a configuration item, an IT service or a process that relies on an alert or notification to discover the current status.
Process	A structured set of activities designed to accomplish a specific objective.
Recovery Time Objective	The maximum time allowed for the recovery of an IT service following an interruption.
Redundancy	Use of one or more additional configuration items to provide fault tolerance. The term also has a generic meaning of obsolescence, or no longer needed.
Resilience	The ability of an IT service or other configuration item to resist failure or to recover in a timely manner following a failure.
Risk	A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred. Risk can also be defined as uncertainty of outcome and can be

	used in the context of measuring the probability of positive outcomes as well as negative outcomes.
Risk Assessment	The initial steps of risk management: analysing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk assessment can be quantitative (based on numerical data) or qualitative.
Service Level Agreement (SLA)	An agreement between an IT service provider and a customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single agreement may cover multiple IT services or multiple customers.
Service Owner	A role responsible for managing one or more services throughout their entire lifecycle. Service owners are instrumental in the development of service strategy and are responsible for the content of the service portfolio.

7. Levels of Operational Importance Relevant to Disaster Recovery.

For services provided by IT Services, the following levels of disaster recovery capability apply:

Disaster Recovery ***(ITIL industry standard names)***	**Level**	**Recovery Time Objective (RTO)**	**Service Recovery Strategy**
Level 0 -Mission Critical A mission critical service requires continuous availability. Breaks in these services are intolerable and immediately cause damage to MU.	MC	< 24 hours	Active/Active A service is run on a primary and secondary server simultaneously with load balancing. If the primary server fails, the secondary server carries the entire service until recovery operations are complete.
Level 1 - Business Critical A business-critical level 1 service requires continuous availability, though short breaks in service are not catastrophic. Availability required for effective business operation.	L1	24 hours (next day)	Active /Active
Level 2 – Business Operational Contributing to efficient business operation but out of direct line of service to customer. Business operational services contribute to the effective running of the company but are out of the direct line of service to customers.	L2	Within 48 hours	Active /Passive A service is run on a primary server with a secondary server in reserve which only engages if the primary server fails.
Level-3 – Administrative Services Services on the level of office productivity tools, required for business to operate. Failures are undesirable but do not affect customers and can be tolerated a little more. Cannot justify extreme additional expenses for higher availability	L3	Within 3 days	Active/Passive

The assets and the systems associated with each particular service shall be identified and clearly defined. The owner for each service shall be assigned and the details of this responsibility documented. This information shall be reviewed and updated at least once per year.

Standard appropriate maintenance contracts for critical components shall be in place.

For each service, the following data shall be maintained by the relevant IT Services Manager.

- Key system data: System owner, service details, backup mechanism, recovery mechanism, system level ranking.
- Key operational procedures for start-up, 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 as required and full-service test schedule.

The following shall also be maintained on the IT Services IT Disaster Recovery Channel:

- Contact lists for IT Services Management and key staff.
- Contacts for key service providers.

8. Relevant Information

IT Services Major Incident and Communications Plan
IT Services Disaster Recovery Plan
Maynooth University Campus Emergency Response Plan
CIIO Risk Register