Disaster Recovery Policy

INTRODUCTION

This policy provides a framework for the ongoing process of planning, developing and implementing disaster recovery management for IT Services at UCD.

A disaster is a serious incident that cannot be managed within the scope of UCD's normal working operations.

DISASTER RECOVERY INCIDENT OPERATIONS INCLUDE:

(a) All activities and steps necessary to restore systems services that are affected by a disaster.

(b) All activities concerned with management and user communications related to the disaster.

(c) All activities concerned with the mitigation of the impact of an ongoing disaster incident.

(d) All activities concerned with the follow-up to an incident.

DISASTER RECOVERY MANAGEMENT

Is the process of planning and preparation to:

- 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.

DISASTER RECOVERY POLICY OBJECTIVES

DISASTER RECOVERY OPERATIONS MANAGEMENT

This policy is implemented to minimise the impact of significant incidents on UCD's services and recover from the unavailability of IT systems to an acceptable level through a combination of responsive and recovery controls.

To achieve this, the following three objectives are set out:

- Establish operational control of the disaster
- Communicate with relevant parties impacted by the disaster
- Activate a specific recovery plan in relation to the disaster

To achieve the above objectives, UCD has decided to align this policy with guidelines set out in ISO 27001: 2005[1], BS 25999[2], and NIST Contingency Planning for IT Systems[3].

The disaster recovery plan is invoked when

- A member of the IT Services management team requests the commencement of DR operations.
- If a critical service sustains a P1 service outage which has lasted 24 hours or is determined as likely to do so.

DISASTER RECOVERY MANAGEMENT PLANNING

To complement this policy, disaster recovery management planning 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 plans shall be made available in a convenient form for use by DR Teams, and shall be reproduced for distribution to all managers periodically as updated to retain for use.

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.

DISASTER RECOVERY PLANNING POLICY

It is neither economical nor practical to maintain fully redundant hardware in preparation for all potential disasters. UCD has implemented cross data centre resilience, where either data centre has the capability to provide adequate operating services to UCD 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.

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 (here referred to as Tier). A service is a collection of systems and devices that collectively support a business process.

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.

[1] ISO 27001:2005 – International Standard for Information Security

[2] BS 25999 – British Standard for Business Continuity Management

[3] National Institute of Standards and Technology (NIST) Contingency Planning for IT Systems - *csrc.**nist**.gov/publications/**nist**pubs/800-34/sp800-34.pdf*

Within UCD, the following levels of disaster recovery capability apply:

Tier	Applicability	Recovery Objective
1	A Tier 1 system is any critical system necessary to support the delivery of primary services by IT Services. Primary services are defined by the CIO, and supporting systems are identified through corresponding analysis.	All Tier 1 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.
2	A Tier 2 system is any other non-critical system operated or managed by IT Services as a production system for University operations.	Tier 2 systems have a design 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.
3	Tier 3: Non-IT Services incidents	These are incidents which involve the loss of use of office facilities by administration or other University staff through a significant unplanned event. In such events IT services facilitate the provision of short term or temporary facilities to accommodate such staff in conjunction with Buildings and Services.

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.

Standard appropriate maintenance contracts for critical components shall 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 System Manager:

- Key system data: System owner, System 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 **IT Security officer** shall be responsible for the collection, management and distribution of the DR Policy and Procedures.

System Managers and delegated systems administrators shall prepare and maintain procedures and plans as required under this policy.

TESTING AND MAINTAINING OF DISASTER RECOVERY PLANS

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 system managers as identified by procedure to ensure that this is carried out in a correct manner.

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

DISASTER RECOVERY MANAGEMENT AND CO-ORDINATION POLICY

Disaster recovery management is incorporated in IT Services processes and structure as follows:- 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 a number of separate teams, which include the following:

1. Disaster Incident Management Team (or Management Team)
2. Recovery Action Team
3. Salvage Team
4. Communications Team

The responsibilities of each team are identified below. Where required this responsibility can be supplemented with more detailed guidance for specific disaster recovery activities. These teams with allocated responsibilities may delegate tasks to appropriate individuals; however they shall ensure that these tasks are correctly performed.

Regular meetings shall be held during the disaster, with regular updates being provided by all teams. Meeting records shall be kept to document the decisions and actions implemented during a disaster recovery.

DISASTER INCIDENT TEAMS

The **Disaster Incident Management Team** (Management Team) shall be primarily involved in making key decisions in relation to the management of the disaster. The team shall consist of

- The Senior Management Team within IT Services,
- Head of Operations
- IT Security Officer (team coordinator)
- Head of Service for Disaster impacted services.
- Head of Customer Services
- Others at the discretion of the management team.

This team is responsible for bringing into play the arrangements for the other teams set out below. They establish milestones and declare when disaster recovery operations are complete. This team will receive status information from the Salvage and Recovery Action teams, and issue instructions to the Communications team.

The handling of communication is vital if the impact of a serious incident is to be minimised and the effects of the incident on reputation are to be significantly reduced. The **Communications Team** shall facilitate the Disaster Recovery Team in addressing, filtering and consolidating both incoming and outgoing communication to the following distinct groups that may be affected by a disaster:

1) The university staff;
2) The students;
3) IT Staff; and
4) Any other external parties;

The disaster recovery communications team shall be the authoritative source for information related to the disaster. Members of all teams shall refer external queries and requests for information to the communications team.

The Disaster Recovery Communication Teams shall liaise with UCD's Communication's Office and Customer Services to ensure all relevant communications channels have been identified.

The team shall comprise the following members:

- Member of Senior Management team (CIO\DCIO)

- Head of Customer Services. (team lead)
- Communications Officer.
- Customer Services line managers.
- Heads of Service not involved in Recovery teams.

The **Salvage Team** shall immediately assemble for the purposes of implementing ad-hoc actions to assess the recoverability of resources and facilities where the disaster has occurred. It is essential that the Salvage Team has activity plans, and outline instructions to act in the various emergencies that are envisaged in order to allow productive engagement with the disaster. This team operates within a doctrine of understanding primary recovery objectives and current capabilities, and aims to re-use remaining and existing capability to aid recovery. The Salvage Team reports to the Disaster Management Team as required.

This team shall comprise:

- Senior IT Services technical staff not primarily involved in recovery actions for the disaster.
- Head of Operations.
- IT Security Officer.
- Data Centre officer (team lead).

The **Recovery Action Team** operate on the basis that the disaster will not be resolved for some time and immediately plan recovery activities in a viable location. The team shall have a detailed list of activities pre -approved to be carried out. This is particularly relevant in the first hours of a disaster.

As this team's efforts are predominantly determined by planning, the team shall not, in general engage in any external communication or non-recovery tasks except to the Management Team, except as necessary to perform their tasks. This team's lead shall also keep the Disaster Management Team informed of progress, status, and plans as required.

The recovery action team shall comprise:

- Technical lead for the service impacted.
- Technical team members from impacted areas.
- Technical team members from related disciplines impacted by the recovery requirements.

SCOPE OF POLICY

This policy applies to all IT Services managed systems.