ICHAS			
Section 9 - Information & Data Management			
Subject:	Procedures Associated with IT Disaster Recovery		
Date Approved by Academic Council:			**July 2021**
Policy Version	1/2021	Date due for Revision	February 2024
Parent Policy	Policy on Data Collection, Usage & Management		

INTRODUCTION

The purpose of these procedures is to ensure that the College complies with the Security Measures for Personal Data provisions of the Data Protection Acts 1988-2018. The aim is to set a clear and transparent framework for the ongoing process of planning, developing, and implementing disaster recovery management for IT Services at ICHAS.

It is important to note that no two IT Disaster scenarios are identical. Therefore, no single set of procedures can anticipate and address every possible circumstance. The procedures contained in this document are intended to serve as guide to the primary resources and actions required in the event of the most likely disaster events. They may not be appropriate in all cases. These Procedures Associated with IT Disaster Recovery are not the single source for all the information that describes ICHAS's ability to survive a disaster including the processes that must be followed to accomplish recovery. Other significant resources include focused Disaster Recovery Plans.

RESPONSIBILITIES

ROLE/ PERSON	
Educational Technology Manager	Assists the IS Manager with identifying compromised data and Recovery of Data associated with the LMS.
Information Systems Manager	The IS manager will co-ordinate all activities associated with an IS systems disaster.

Definitions

Disaster: An IT disaster is a major incident that cannot be managed within the

scope of ICHAS's normal Information Systems working operations.

Disaster Recovery (DR): Involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology systems following a disaster.

Information System (IS): Any system or service that transports, processes, and/or stores ICHAS data.

Emergency Management Team (EMT): An ICHAS cross-functional response team that manages potential and/or actual large-scale outages; a published Disaster Recovery Procedure governs the activities of this team.

Recovery Time Objective (RTO): Represents the maximum amount of time an institution can tolerate the loss of an application or, conversely, how quickly an application must be restored to working order in the event of a disaster.

Recovery Point Objective (RPO): Represents the maximum amount of data loss an institution can tolerate for a given application in the event of a disaster.

Risk Assessment (RA): Initial steps of risk management which analyzes the value of the IT assets to the college, identifying threats to those IT assets, and evaluating how vulnerable each IT asset is to those threats.

Virtual Private Server (VPS): Managed cloud-based servers. Hardware and OS maintained at source. Applications and Data controlled directly by ICHAS.

Service Level Agreement (SLA): Guarantees of server uptime and software availability agreed by VPS service providers.

Procedures Associated with IT Disaster Recovery

1. Risk Assessment

Formal risk assessments and impact analysis are carried out on an annual basis when significant infrastructure change demands, by the IS manager in consultation with the Information Technologist and contracted external support experts. These assessments are utilised in identifying specific systems at risk and likely threats that could cause an IT disaster and reported to the Vice President for Corporate affairs and the Vice President for academic affairs.

The following systems at ICHAS are identified as potential risks:

- College Client/Server Network and file systems
- The Learning Management System (LMS)
- The Student Information System (SIS)

The following are identified as possible major threats to ICHAS systems:

- College hardware or software systems failure
- Cloud-based LMS systems hardware or software failure
- Cyber attack

2. Systems Audit

An audit of the college IT infrastructure is carried out annually. This has identified all hardware and software resources, on-site and cloud-based, utilised by each of the major IT systems identified.

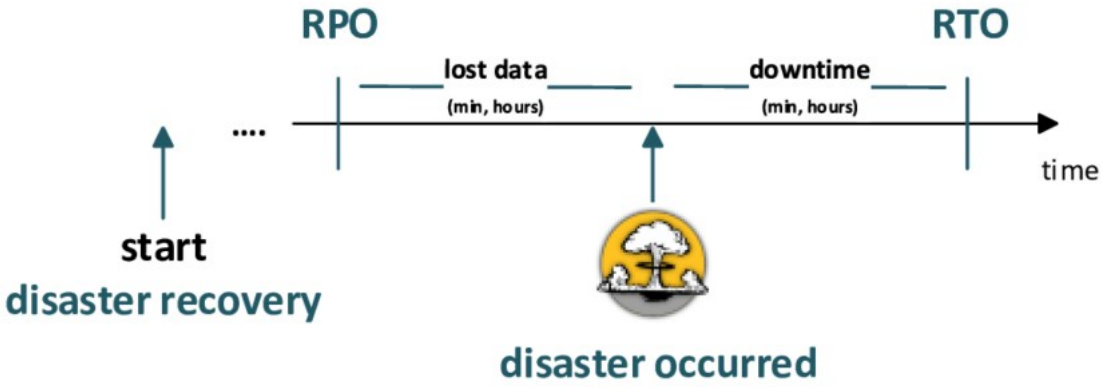
3. Disaster Recovery Team

In the case of an IT disaster a team is constituted to deal with such an event. The following table details the makeup of the ICHAS disaster recovery team and some of their responsibilities. The constituted team embodies a substantial range of knowledge and expertise across the information technology fields. As and when required Incident Teams will be drawn from this group.

Team Member	**Responsibilities/Function**
IS Manager	• Primary contact for notification of incident • Assess the nature and impact of the event. • Manages the implementation of the appropriate Disaster Recovery Plan • Acts as a resource
Educational Technology Manager	• Assists with identifying compromised data. • Recovery of Data associated with the LMS.
Moodle Technology Expert	• Moodle Platform recovery • Cloud-based server configuration services
IT Support Technicians	• On site server hardware and software recovery • Cloud-based systems support • Data recovery
NTES	• Contracted external support services. • On site server hardware and software recovery • Hardware Firewall configuration • Consultation services
Vice President of Corporate affairs	• will liaise with the IS Manager and the College management team to ensure that key roles and responsibilities are coordinated, and that all available information is available to address the disaster.

4. Determine Response Approach for Each Service

Using the list of technology services identified in the Risk Assessments and Impact Analysis from Section (1.): ICHAS has established Planning Priorities to determine the preventative measures for each service, and recovery options for each service. The following factors are considered when determining the technical approach:



Recovery time objective (RTO) and recovery point objective (RPO): Services with a short recovery time objective or recovery point objective are more likely to require a combination of preventative and recovery approaches, to meet the college's organizational needs.

5. Risks and risk mitigation strategies

Each service faces numerous risks, which would be time consuming to identify and mitigate. The college felt it more effective to develop a strategy for handling each of the major risk scenarios. This approach will address the majority of risks to a service. The following table exemplifies this approach:

IT Service	Risk Scenario	Recommended Technical Approach
College Client/Server Network and file systems **On-Site**	Loss of Facility Through Hardware Destructive/ Non-Destructive Event	**Preventative:** Regular server maintenance and update schedules. Replacement contracts for major equipment and redundancy replacements for network infrastructure. **Recovery:** Repair or replacement of failed hardware. Server software systems images maintained on-site and cloud-based. Preventative facility will function as primary facility.
	Loss of Facility Through Software Destructive/ Non-Destructive Event	**Prevention:** All operating system and application software kept up to date. Regular diagnostics and monitoring of server logs. **Recovery:** Recover data from local and cloud-based backup. Recovery facility will function as primary facility.
	Loss of Facility Through Cyber Attack	**Preventative:** Hardware and software Firewalls to be primary protection against brute force attack. Secondary protection offered by server and workstation Security Software. Staff training in security best practices. **Recovery:** Recover data from local and cloud-based backup. Long term backups maintained for recovery from severe attack e.g. Ransomware. All backups encrypted. Preventative facility will function as primary facility.

IT Service	Risk Scenario	Recommended Technical Approach
Learning Management System (LMS) **Cloud-Based**	Loss of Facility Through Hardware Destructive/ Non-Destructive Event	**Preventative:** World class VPS maintained in regional Data Centre. Comprehensive SLA's **Recovery:** In the unlikely event of failure, a new server can be spun up and operational within 30 min. Recover data from cloud-based backup. Backups maintained across different data centres. Preventative facility will function as primary facility.
	Loss of Facility Through Software Destructive/ Non-Destructive Event	**Prevention:** All operating system and application software kept up to date. Regular diagnostics and monitoring of server logs. **Recovery:** Recover data from cloud-based backup. Backups maintained across different data centres. Recovery facility will function as primary facility.
	Loss of Facility Through Cyber Attack	**Preventative:** Service providers to ensure protection against brute force attack utilizing industry leading hardware and software Firewalls. Secondary protection offered by server Security Software. Staff training in security best practices. **Recovery:** Recover data from local and cloud-based backup. Long term backups maintained for recovery from severe attack e.g. Ransomware. All backups encrypted. Preventative facility will function as primary facility.
Student Information System (SIS) **Cloud-Based**	Loss of Facility Through Hardware Destructive/ Non-Destructive Event	**Preventative:** World class VPS maintained in regional Data Centres. Comprehensive SLA's **Recovery:** In the unlikely event of failure, a new server can be spun up and operational within 30 min. Recover data from cloud-based backup. Backups maintained across different data centres. Preventative facility will function as primary facility.
	Loss of Facility Through Software Destructive/ Non-Destructive Event	**Prevention:** All operating system and application software kept up to date. Regular diagnostics and monitoring of server logs. **Recovery:** Recover data from cloud-based backup. Backups maintained across different data centres. Recovery facility will function as primary facility.
	Loss of Facility Through Cyber Attack	**Preventative:** Service providers to ensure protection against brute force attack utilizing industry leading

IT Service	Risk Scenario	Recommended Technical Approach
		hardware and software Firewalls. Secondary protection offered by server Security Software. **Recovery:** Recover data from local and cloud-based backup. Long term backups maintained for recovery from severe attack e.g. Ransomware. All backups encrypted. Preventative facility will function as primary facility

The results of sections (1.),(2.), and (4.) will inform the detailed content of this table and contribute to the associated IT Disaster Recovery plans.

6. Disaster Recovery Plans

Based upon the results of the Risk assessment and Impact Analysis reports, and in conjunction with the determined response approaches and mitigation strategies:

a. The college has developed a comprehensive Strategic Disaster Recovery Plan
b. Individual Disaster Recovery Plans were developed to cater for each identified IT Service, to include each identified major risk scenario.
c. The specific hardware and software resources associated with each individual plan are identified and included in the plan details.
d. All recovery plans are published to an agreed location with all relevant staff provided with access details and access rights.

7. Systems and Data Backup

Based on the risk assessment and mitigation strategies the following backup and data retention procedures were implemented:

- In the case of each identified college IT Service primary data backups are scheduled on a daily basis. Production data will never be more than 24 hours old. 7 Day copies are retained.
- In the case of each identified college IT Service system operating software is backed up on a weekly basis. 3 Copies are retained.
- In the case of each identified college IT Service the complete server is replicated by snapshot. This provides a technically complete mirror copy of all server content. This is completed monthly. 3 months copies are retained. This is maintained as a precaution against a major Cyber-attack.

8. Testing and Review

Simulations are scheduled to test failure scenarios and recovery process in real time. This is to ensure that the process associated with each of the developed IT Disaster Recovery plans work and that data and systems can be recovered according to planned time scales. Results of testing are reviewed, and changes made were necessary.

9. Staff Training

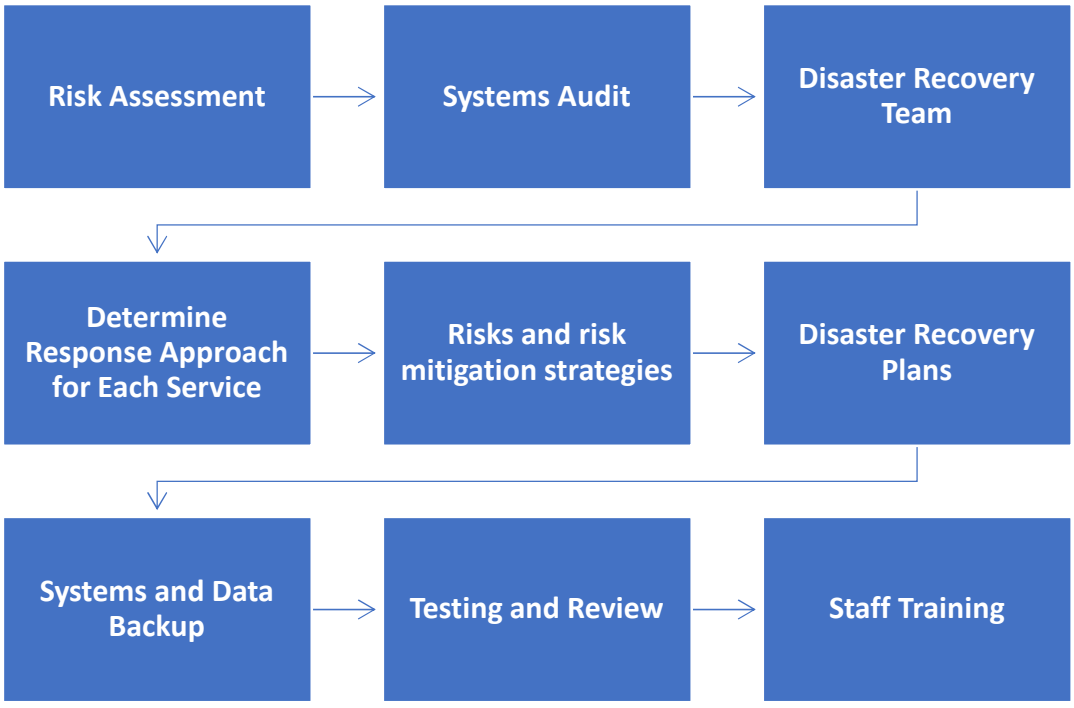
Each member of the IT Disaster Recovery Team is trained in the relevant aspects of each of the specific disaster recovery plans, associated with their roles.
Non-IT Staff are provided with training in general and specific preventative measures associated with each of the IT Systems they engage with**.** As part of their induction, they also receive awareness training centered on disaster recovery.

10. Response Procedure

The following represents a brief outline of the core procedures associated with an IT disaster event.

1. The IS Manager is notified of the event.
2. The IS Manager will perform an initial assessment of the nature and impact of the event, to identify:
    a. Which IT Facility has been impacted.
    b. The nature of the disaster (Hardware/Software Failure, Cyber Attack)
3. Based upon the initial assessment an incident team will be formed from the members of the Disaster Recovery Team.
4. The Incident Team will further assess the disaster incident and select the appropriate pre-determined Disaster Recovery Plan.
5. Incident Team implements the recovery plan.
6. The IS Manager will produce a full incident report post recovery.

Graphical Representation of the Procedure



Linked Policies	Policy on Data Collection, Usage & Management
Linked Procedures	Procedure associated with on Data Collection, Usage & Management