Section 9 – Policy Associated with Information and Data Management

Subject:	Disaster Recovery Policy		
Applicable QQI Core Standard	Information and Data Management		
Date Approved by Academic Council:			**June 2021**
Policy Version	1/2021	Date due for Revision	February 2024

CONTEXT

The Data Protection Act (1988/2018)

This principle, as set out in the Data Protection Act, is applied to all data processed at ICHAS:

72. (1) In determining appropriate technical or organisational measures for the purposes of section 71 (1)(f), a controller shall ensure that the measures provide a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, the data concerned.

POLICY STATEMENT

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

SCOPE

Applies To	**Staff**	**Students**	**Both**	
	✓			
Responsible for Implementation	Data Protection Officer			
Responsible for Monitoring & Review	Vice President (Academic Affairs)	IS Manager	Data Protection officer	Registrar
			✓	

Definitions

Data Subject - If an organisation or company is holding or using your personal data, you are known as a **data subject**.
Data Protection Officer (DPO) - A data protection officer (DPO) is a position within the College who acts as an advocate for the proper care and use of Personal information.
Data Controller - A 'controller' refers to a person, company, or other body that decides how and why a data subject's personal data are processed.
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 transport, 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

OVERVIEW

Disaster Recover 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 procedures:

- Emergency response procedures to document the appropriate emergency response to IT hardware failure, cyber-attack, or any other activities in order to protect data and limit systems damage.
- Backup operations procedures to ensure that essential data processing operational

tasks can be conducted after the disruption.

- Recovery actions procedures to facilitate the rapid restoration of a data processing system following a disaster.

DISASTER RECOVER POLICY

1. The college shall develop comprehensive disaster recovery plans in accordance with good disaster recovery management practices
2. Technology disaster recovery activities shall be performed as part of the college's Information Systems Management to include:
    a. Planning and design of IS disaster recovery activities, which include technology disaster recovery plans.
    b. Identification of DR teams, defining their roles and responsibilities and ensuring they are properly trained and prepared to respond to an incident.
    c. Scheduling of updates to DR business impact analyses.
    d. Scheduling of updates to DR risk assessments.
    e. Planning and delivery of awareness and training activities for employees and DR team members.
    f. Planning and design of incident response activities.
    g. Planning and execution of DR plan exercises.
    h. Designing and implementing a DR program/plan maintenance activity to ensure that all plans are up to date and ready for use.
    i. Preparing for management review and auditing of DR plans.
    j. Planning and implementation of continuous improvement activities for the DR program and plans.
3. A formal risk assessment (RA) and business impact analysis (BIA) shall be undertaken to determine the requirements for all DR plans; RAs and BIAs shall be updated at least annually to ensure they are in alignment with the college activities and its technology requirements.
4. Strategies for responding to specific technology disaster incidents shall be identified, and used when developing individual DR plans.
5. Disaster recovery plans shall address critical technology elements, including systems, networks, databases, and data, in accordance with key college activities.
6. Disaster recovery plans shall be periodically tested in a suitable environment to ensure that the systems, networks, databases, and other infrastructure elements can be recovered and returned to a business as usual (BAU) status in emergency situations and that ICHAS management and employees understand how the plans are to be executed as well as their roles and responsibilities.
7. All employees must be made aware of the disaster recovery program and plans and their own roles and responsibilities during an incident.
8. Technology disaster recovery plans and other documents are to be kept up to date and will reflect existing and changing circumstances.

9. 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 college process.
10. 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 if recovery is required.
11. The critical nature and recoverability of specific data will determine the Recovery Point Objective (RPO)

Disaster Recovery Planning

As it is not practical, or economical, for the college to maintain completely redundant systems to cater for DR, the recovery of hardware or services will be determined by their critical status. This will indicate by an agreed RTO for each service.

The following represents the levels of DR capability at ICHAS

SYSTEM	**RECOVERY OBJECTIVE**
1. Critical on-site systems needed to support the delivery of ICHAS primary IT services	These systems are highly resilient across dual-data centres. The design recovery time objectives (RTO) for these systems are a maximum of 24 hours. The minimum essential services for all critical systems are identified and documented.
2. Critical cloud-based systems needed to support the delivery of ICHAS primary IT services	These systems have a design maximum recovery time objective (RTO) of 4 hours, and all minimum essential services are identified to ensure efficient recovery. Data shall be recoverable from cloud-based backup storage media, and where necessary and feasible, full systems shall be backed up.
3. non-critical system operated or managed by IS Services as a production system for ICHAS operations	These systems have a design maximum recovery time objective (RTO) of 48 hours, and all minimum essential services are identified to ensure efficient recovery. Data shall be recoverable from cloud-based backup storage media.
4. Third party noncritical systems not directly managed by IS services at ICHAS	Recovery of these services will be based upon SLA

Linked Policies and Procedures

Linked Policies	Policy on Data Collection, usage, and Management
Linked Procedures	Procedures associated Data Collection, usage, and Management. Procedures associated IT Disaster Recovery