SERC

INSPIRING. TRANSFORMING. ENRICHING.

POLICY TITLE

Information Technology & Services (ITS) Disaster Recovery Policy

Academic Year: 2021/22 onwards

Target Audience:

All Staff and Governors

Summary of Contents:

This Policy sets out the College's plan on maintaining and restoring critical IT services in each main College Campus, in the event of an IT disaster. The Policy focuses on responses to disaster level outcomes (e.g. loss of one or more services such as Telephones, Active Directory, Student Records or information systems for prolonged periods) rather than causes of disaster situations (e.g. fire in a data centre).

Enquiries: Any enquiries about the contents of this document should be addressed to:

Title:	Chief Technology Officer
Address:	Bangor Campus Castle Park Road Bangor BT20 4TD
Tele:	028 9127 6600 X 8205
Mobile:	07899958209
E-mail:	aemmett@serc.ac.uk

Approval by:

CMT – 8 June 2020

Audit Committee – 17 June 2020

Governing Body – 29 June 2020

Policy Number: 055-2019

First Created:	February 2019
Last Reviewed:	June 2020 June 2021 June 2022
Next Review Due:	June 2024

Related Documents:

Information Technology & Services (ITS) Disaster Recovery SOP

College Business Continuity Plan

Superseded Documents (if applicable):

Equality of Opportunity and Good Relations Screening Information (Section 75):

Date Procedure Screened – 20/02/19

Contents

1.0 Change History

Changes to this SOP are documented in Appendix 1 of this document. When reading electronic copies of this document, you may click here to view the change history.

2.0 Abbreviations

The definition of abbreviations used within this policy are as follows:

CMT (College Management Team)

The senior management team within the College.

College Computing Services

Defined as any item of computing equipment, (i.e. PCs, macs, laptops, MacBook’s, tablets, mobile phones, servers) or software services owned by SERC.

ICSC (Information & Cyber Security Committee)

The committee responsible for monitoring cyber & information security within the college.

ITS (Information, Technology & Services)

The college department responsible for the delivery of computing services at SERC.

JANET (Joint Academic NETwork)

The trademark used for the collection of networking services and facilities which support communication requirements of the UK education and research community. This service is provided by JISC.

JISC (formerly the Joint Information Systems Committee)

The UK higher, further education and skills sectors’ not-for-profit organisation for digital services and solutions. It operates shared digital infrastructure and services, negotiates sector-wide deals with IT vendors and commercial publishers & provides advice and practical assistance for universities, colleges and learning providers.

3.0 Introduction and Scope

South Eastern Regional College has an ICT infrastructure that spreads over four main campuses:

- Bangor
- Newtownards
- Downpatrick
- Lisburn

There are several smaller satellite sites which also connect back to a primary Campus. Focus in terms of disaster recovery planning, will be on maintaining and restoring critical ICT services in each main Campus.

The policy focuses on responses to disaster level outcomes (e.g. loss of one or more services such as Telephones, Active Directory, Student Records or information systems for prolonged periods) rather than causes of disaster situations (e.g. fire in a data centre).

This Policy forms the basis for the ITS Disaster Recovery SOP and should also be read in conjunction with the College's Business Continuity Plan.

In preparing this policy the following assumptions have been made:

1. All non-essential work will cease immediately following a disaster. This will free up ITS resources to implement the Disaster Recovery (DR) plan.
2. People will be released to enact the recovery and computer resources may, if required, be reconfigured or reallocated or to replace lost production services.
3. The policy and plan is expected to cater for only one disaster level event at any one time.

4.0 Roles and Responsibilities

The Chief Technology Officer is responsible for ensuring that appropriate policy, plans and procedures are in place to restore ITS facilities in the event of a major failure or disaster. In addition, they are responsible for ensuring that the "out of hours" staff rota is adequately maintained to support the plan outside of normal business hours.

As part of the colleges Business Continuity Plan (BCP), the Chief Technology Officer and the Managers responsible for each Service must carry out assessments on each Service to measure the realistic impact a failure would have on the college. They should develop and improve the DR procedures to manage this impact and communicate the risks and mitigation steps planned.

The Head of Networks is responsible for ensuring that the computer systems including applications and data are backed up as stated in the Backup Policy.

The Chief Technology Officer is responsible for ensuring that the data network is designed for resilience and maintained with adequate capacity as required in this policy.

A role of 'Disaster Recovery Plan Lead' exists within the DR SOP and responsibilities are defined within the SOP. This role will be filled by the most senior ITS manager on-site during normal office hours or initially by the on-call ITS manager outside of normal business hours.

5.0 Process for Implementing this Policy Document

5.1 Approach

Enough capacity will be maintained in the core network and in computer and communications rooms (including air conditioning, power, and floor space) to recover from the loss of one room within target timescales.

Each service provided by the ITS will be classified by business criticality in line with the table below. There will be a four-tier classification of services each with a target recovery timescale.

There will be a process to categorise each service by cost and benefit of rapid recovery.

Category	Recovery Time	Examples
Category 1	< 1 Hour	Core Infrastructure including Network Switches, Firewalls, Internet Connectivity & Identity Services.
Category 2	< 1 Day	Primary Line of Business Systems including HR, Finance, Student Records & VLE
Category 3	< 5 Days	Secondary systems such a file servers, library information systems and in-house applications.
Category 4	< 14 Days	Equipment acting in a failover role that will require a procurement exercise, but the loss of which will not affect the delivery of services.

A detailed step by step DR plan will be maintained and periodically tested of how recovery will be enacted using the individual recovery procedures including:

1. Switching to dedicated failover equipment where it exists
2. The re-assignment and reconfiguration of development systems to support production systems for which resilient hardware does not exist
3. Procurement arrangements for equipment, software or contract services to recover less critical systems

Capacity planning processes will be run regularly ensure that DR capacity is maintained in line with developments and enhancements on the production environment.

Following a disaster level event this policy assumes that all development, training and other non-live (non-production) work will be suspended.

The recovery policy will encompass re-instating services following a disaster at DR locations. Any reinstatement works, such as rebuilding, to allow a return to normal operations is outside the scope of this policy.

5.2 Risk Assessment

A procedure will be applied to each college service and each new service during development, to assess the following:

1. How long can the college afford to be without the service?
2. What would happen if no pre-disaster preparations are made?
3. What is the hourly cost of being without the service?

From this assessment, a Category level will be assigned to each service in line with the table in section Approach of this document. This Category assignment will then drive investment in pre-disaster preparations for that service and the environment in which it resides.

5.3 Alignment with College Business Continuity Plans

It is important to recognise that a Disaster Recovery plan alone is insufficient to guarantee continuity of operations following a DR level event. The ITS DR plan is one element of a wider College Business Continuity Plan (BCP). To ensure that these different plans remain synchronized, the ITS DR plan will be tested as part of the wider college BCP process.

5.4 ITS Disaster Recover Standard Operating Procedure

The ITS Disaster Recovery SOP on the Learning Engine on the Staff Intranet contains further detail on the College's DR plan. Additionally, further detail is included within the College's Business Continuity Plan located on the Campus Management team site.

6.0 Testing

Testing of the DR plan will be undertaken on a selected subset of college provided services at least annually. The selected subset will vary from year to year. Testing will take place in January/February.

7.0 Communication

This Policy will be available for all users via College intranets and public Website. It will be made available, on request, in alternative formats including large print, braille, audio, and in minority languages to meet the requirements of those who are not fluent in English.

8.0 Review

This policy will normally be reviewed biennially, however if changes are required outside of this cycle to reflect changes in circumstance, this policy will passed through the relevant approval processes at the earliest opportunity.

Appendix 1: Document Change History

Date of Change	Approved By	Change Detail
February 2019	AE	Created
June 2020	AE	Amendments Made to: 1. Section 3 – Spelling correction 2. Section 8 – Updated review cycle text
June 2021	AE	Reviewed in June 2021 – no amendments required
01/06/2022	AE	Amendments made: 1. Converted bulleted lists to numbered lists for easier referencing 2. Moved change history to end of document. 3. Review date changed to every two years.