Procedure Title:	IT Business Continuity and Disaster Recovery Procedure
Procedure ID:	6-605A
Manual Classification:	Section 6 – ITS
Linked to Policy:	6-605 IT Business Continuity Policy
Approved by Senior Management Team:	March 2022
Revision Date(s):	March 2022
Effective Date:	July 1, 2022
Next Review Date:	June 2025
Contacts for Procedure Interpretation:	CTO Directors, Information Technology

1.0 – Purpose

The purpose of this procedure is to ensure that, in the event of a disaster, the College has appropriate and efficient plans in place to address business continuity. The objective is to ensure the timely recovery and return to service of all business-critical IT resources.

2.0 - Definitions and Acronyms

Application or System Administrator	Any user who manages the upkeep, operation, and configuration of an electronic system or application. These users can be identified by having administrative privileges over the system or application.
Business Continuity (BC)	The capability of an organization to continue the delivery of products and services within acceptable time frames at a predefined capacity during a disruption.
BCMS	A Business Continuity Management System provides appropriate operating capabilities and response structure to ensure availability and business continuity of electronic data, information systems, and IT infrastructure.
Business Continuity Plan (BCP)	Documented information that guides an organization's response to a disruption in order to recover, restore and resume the capacity to operate consistent with the business continuity objectives.
CTO	The Chief Technology Officer is the College's executive role responsible for the management, implementation, and usability of information and computer technologies across the College. The CTO is responsible for all technology solutions purchased, configured, delivered, and used across the College, ensuring high availability, functionality, information security, and privacy.
BC/DR	Business Continuity and Disaster Recovery is a set of processes and techniques used to help an organization recover from a disaster and

	continue or resume normal operations. It is a broad term that combines the roles and functions of IT and the rest of the organization in the aftermath of a disaster.
Data Trustee	A senior administrative employee that has responsibility for a functional area of the College and any records related to that function. The Data Trustee is accountable for ensuring that its records are maintained according to College policy. (See related definition of Office of Primary Interest).
Disaster Recovery Plan (DRP)	A plan that defines how an organization's IT department will recover from a natural or human-made disaster. The processes within typically include server and network restoration, copying backup data, and provisioning backup systems.
ERM	Enterprise Risk Management
IT	Information Technology
ITS	Information Technology Services is the full name of Fleming's IT Department.
Office of Primary Interest (OPI)	In alignment with the Canadian Library and Archives, the OPI is the office or department that has the main responsibility for a subject area and any related records. The OPI, as the primary Data Trustee, is accountable for ensuring that its records are maintained according to College Policy, Operating Procedures, and Standards. For example, the department responsible for the recording of minutes by a committee would be considered the OPI and must ensure that those records are properly classified and protected.
RPO	The recovery point objective (RPO) is the maximum acceptable amount of data loss measured in time. It is the age of files or data in a backup that are restored when needed, for example, one day.
RTO	The recovery time objective (RTO) is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operation and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable.
SMT	Senior Management Team

3.0 – Guiding Principles

A comprehensive backup process and associated schedules must be established and maintained regularly for restoring critical data and services in the event of a disaster, up to a specified recovery point objective (RPO) for each critical IT system.

The CTO will appoint a Business Continuity & Disaster Recovery (BC/DR) Team with defined responsibilities and schedules.

System and Application Administrators will develop, maintain, and test plans to backup and restore systems and data, as part of operational due diligence and DRP testing, for the respective systems under their custody and control.

Backups must utilize read-only or immutable data technology to protect backup resources.

Offsite copies must be maintained to ensure resilience from site or location-specific disasters.

If and when needed, invocation of a disaster recovery response is a top priority for the College with significant efforts focused on the recovery and restoration of data and services within the RTO timeframe. During this time access to other IT services or systems may be limited. Resources may be reassigned as required in consultation with SMT.

4.0 – Operating Procedure

4.1 Governance and Plan Development

The CTO will appoint a Business Continuity & Disaster Recovery (BC/DR) Team with defined responsibilities and schedules. The BC/DR Team is responsible for:

- identifying all business-critical IT systems and resources;
- deliver an overall disaster recovery plan (DRP) and strategy;
- deliver and maintain a disaster recovery plan (DRP) for each business-critical IT system, resource, or site;
- prioritization of systems, data, and services to be recovered in the event of a disaster;
- schedule DRP testing;
- schedule a DRP review on an annual basis;
- provide updates to SMT on the status of BC/DR Team activities and performance assessment of disaster recovery plans.

The Business Continuity & Disaster Recovery (BC/DR) Team will review the risks and business criticality of the system and prioritize the development and maintenance of an appropriate disaster recovery plan (DRP) and associated schedule.

Each disaster recovery plan (DRP) must include:

a) a defined scope;
b) identification of critical business functions and their dependencies on IT resources and systems;
c) a risk assessment and business impact assessment;
d) establishment of a recovery point objective (RPO) and recovery time objective (RTO);
e) data backup and recovery plan;
f) a disaster declaration procedure that identifies criteria used for declaring a disaster and a notification procedure;
g) consideration for offsite requirements and capabilities, and agreements in place where necessary;

h) consideration for the security of backup resources and data transit;
i) establishment of a disaster recovery team (DRT) that oversees and executes the disaster recovery plan in the event of a disaster declaration;
j) Review and acceptance by the OPI.

4.2 Backup and Restore Processes

The status of all backups must be recorded daily and reviewed each business day, at a minimum. Backup failures will be treated as an IT incident anytime there is the potential for data loss and/or the RPO is at risk. Backup incidents will be escalated and prioritized based on the system criticality and the elapse time since the last regularly scheduled backup.

Change to backup schedules and job definitions will following the ITS change management process.

During the commissioning of a new College system, application or data resource, a backup and restore plan must also be implemented prior to transitioning into active service.

The College administrative employee responsible for overseeing the commission of a new system, application or data resource is also responsible to:

a) work with the System/Application Administrator and ITS staff to ensure that backup and restore plan have been implemented;
b) inform the Business Continuity & Disaster Recovery (BC/DR) Team of the new service or change.

5.0 – Related Documents

- College Policy #6-605, IT Business Continuity Policy

History of Amendments & Reviews

N/A