FLEMING

Policy Title:	IT Business Continuity Policy
Policy ID:	6-605
Manual Classification:	Section 6 – Information Technology
Approved by:	Board of Governors
Revision Date(s):	June 2022
Effective Date:	July 1, 2022
Next Policy Review Date:	June 2025
Contacts for Policy Interpretation:	CTO Directors, Information Technology

1.0 - Policy Overview

This policy (the "**Policy**") describes how the College will take the necessary steps to prepare for a disaster that impacts the business continuity of the College as supported by the College's information technology (IT) resources and services.

2.0 - Purpose

The purpose of this Policy 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.

3.0 - Definitions and Acronyms

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.
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.
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.
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.
RPO	The recovery point objective (RPO) is the maximum acceptable amount of data loss measured in time. It is the benchmark for backup frequency and represents the worst case of data loss assuming regular backups are successfully completed, so for an RPO of one day, daily backups would be completed.
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 acceptable duration of a systems and data recovery process because after this time the consequences of the interruption become unacceptable.
SMT	Senior Management Team

4.0 - Scope

This policy provides assignment for BC/DR responsibility for critical business processes using information technology.

5.0 - General Principles

5.1 The Chief Technology Officer (CTO) is accountable for the availability and business continuity of all information technology resources operated by the College.

5.2 The IT Directors are responsible for the development, maintenance, management, and execution of the College's Business Continuity Management System (BCMS).

5.3 Fleming College will adopt ISO-22301, "Security and resilience – Business continuity management systems – Requirements", as a standardized framework for implementing and maintaining a BCMS.

5.4 A risk-based approach to IT business continuity planning, aligned to the College's Enterprise Risk Management Policy, will provide risk oversight and internal controls for identifying and managing College risks in line with the activities and reporting functions of the ERM Committee.

5.5 Data archive, data retention, and source document retention policies and practices must enable full data recovery in the event of a disaster in addition to other business and legal requirements governing data retention.

5.6 The CTO will appoint a Business Continuity & Disaster Recovery (BC/DR) Team responsible for identifying all business-critical IT systems and disaster recovery planning.

5.7 SMT will support the implementation of the BCMS and related BC/DR Team activities by:

a) Making informed decisions on risk tolerances and acceptable levels of operation impacts to the College in various potential disaster scenarios.
b) Provide appropriate levels of resources and investment to achieve the desired capabilities and outcomes.
c) Directing stakeholders to support and contribute to BCMS and BC/DR Team activities.

6.0 - Related Documents

- College Policy #1-108, Enterprise Risk Management
- Operating Procedure #6-605A OP, IT Business Continuity and Disaster Recovery
- International Organization for Standardization, Security and resilience – Business continuity management systems – Requirements - ISO 22301

History of Amendments/Reviews

Original approved June 2022