OFFICE OF INFORMATION TECHNOLOGY
BUSINESS CONTINUITY & DISASTER RECOVERY

I. PURPOSE AND SCOPE

This rule supports the Information Security Policy Section IV.J: "Business Continuity and Disaster Recovery Planning."

II. DEFINITIONS

A. **Information Asset:** data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling the college to perform its business functions.

B. **Information System:** an application or group of servers used for electronic storing, processing, or transmitting any college data or information asset.

III. PROCEDURES

A. The Office of Information Technology (OIT) will ensure the Business Continuity and Disaster Recovery plans (the plan) include the following information security requirements:

1. identification and prioritization of college essential business processes;
2. inventory of personnel, information assets and information systems involved in essential business processes;
3. understanding of impact of natural and facility threats on the safety of users and essential business processes
4. understanding of impact of information security incidents on essential business processes;
5. identification of resources required to address any identified information security requirements to mitigate the impact of information security incidents on essential business processes;
6. identification of personnel roles and responsibilities with regards to business continuity and disaster recovery procedures; and
7. implementation of business continuity and disaster recovery procedures that support the safe and timely recovery and restoration of essential business processes.

B. Business Continuity and Disaster Recovery Supporting Procedures must include the following information security requirements:

    1. conditions for activating the business continuity and/or disaster recovery plans;

    2. plan roles and responsibilities for execution;

    3. actions to be taken under the following conditions:

        a. Emergency: following a disaster or security incident which interrupts or jeopardizes business operations.

        b. Failover: temporarily moving essential business processes to pre-established alternative locations and restoring operations in the required time frames.

        c. Resumption: returning to normal business operations.

C. The college will, with full involvement of business process owners, complete a business impact analysis, including:

    1. identifying events that interrupt essential business processes;

    2. formally capturing the likelihood and impact of these interruptions and their consequences to information security; and

    3. assigning criticality tiers for applications and information systems that support associated business processes.

D. OIT will test and update the plan biannually using a variety of the following techniques:

    1. table-top discussions and hypothetical testing of likely scenarios;

    2. scenario simulation;

    3. technical recovery testing with actual shutdowns;

    4. alternate site activation testing; and

    5. complete biannual rehearsals.

E. OIT will update revisions to the plan from lessons learned.