Policy 1206
Contingency Management for Technology-based Information Systems

Date of Current Revision: February 2024
Responsible Officer: Associate Vice President for Information Technology and CIO

1. PURPOSE

This policy establishes the requirement for departments to create and maintain written contingency management plans for all technology-based systems/applications that support critical functions.

2. AUTHORITY

The Board of Visitors has been authorized by the Commonwealth of Virginia to govern James Madison University. See Code of Virginia § 23.1-1600; § 23.1-1301. The Board has delegated the authority to manage the university to the president.

3. DEFINITIONS

Business Impact Analysis
Examining the relationship between key business processes of the university and its ability to sustain and execute critical functions. Business impact analysis also identifies the technology resources required to sustain such critical functions.

Contingency Management Plan
A plan that includes the identification of critical functions, an inventory of the backup facilities, and other information technology resources required in the event of a contingency, procedures for alternative processing and recovery, and requirements for training, testing, and maintenance related to the plan.

Critical Functions
Business processes identified by the vice presidents that significantly affect service levels to students, affect public safety, impact the budget, and/or are the result of governmental regulations; those functions of information systems that are so important to the university that their loss or unavailability is unacceptable. With a critical function, even a short-term unavailability of the information provided by the system would have a significant negative impact on the fiscal or legal integrity of university operations, or on the continuation of essential university programs/services.

Information System
A set of processes and resources to generate, manipulate, store and/or disseminate data. Information systems are usually part of a larger business function and generally take one of the following three forms:

- Central information systems:
  Information systems that use central computing facilities, the central communications network, and/or other shared resources and are managed by Information Technology (IT).

- Local information systems:
  Information systems that use only individual workstations and/or departmental server resources not managed by IT.

- Manual information systems:
  Information processes that use no information technology/electronic automation.

System Owner
The individual responsible for overall functionality of an information system and for appropriate stewardship of the data it includes. The System Owner works in cooperation with IT to evaluate, license, and implement the system and establish necessary controls to ensure appropriate functionality and security are achieved. In some cases, the System Owner may also be a Data Custodian.

4. APPLICABILITY

This policy applies to all critical functions supported by technology-based information systems, applications, or services.

5. POLICY

Departments must have contingency management plans in place and detail how critical functions will be performed, should a contingency event result in the absence of normal facilities, information resources, or personnel. IT must have a contingency management plan for the central computing facilities and the communications network. The plans will also outline the procedures to be used for returning to a normal operating environment. The development and maintenance of contingency management plans must adhere to university policies and standards, including that all or part of the plans' contents be tested annually to ensure that they are complete, current, and workable. Testing should be done in a manner that will not interfere with the normal quality of university services.

6. PROCEDURES

6.1 Annually Information Technology will request the evaluation of critical functions by the Vice Presidents.

6.2 Adequate written contingency management plans must be developed and maintained for all technology-based information systems that support critical functions. The contingency management plans must be reviewed, tested, and updated at least annually, and all personnel affected by the plan adequately trained on the content and operation of the plan.

6.3 Vice Presidents will:

- Inform departments within their divisions of the critical functions
- Inform IT of the critical functions within their division
- Ensure that adequate contingency management plans are in place for critical functions
- Ensure that departments have established alternate procedures to be used during a recovery period for central information systems
- Decide when situations require the activation of contingency management plans and/or alternate procedures

6.4 Deans, associate/assistant vice presidents, directors, and academic/administrative unit-heads will:

- Develop and maintain contingency management plans for local and manual information systems
- Establish alternate procedures necessary to sustain functionality during the recovery period for central information systems
- Periodically review, test, and update contingency management plans and alternate procedures
- Ensure that personnel within their areas are adequately trained on the contents of the plans

7. RESPONSIBILITIES

Vice presidents are responsible for identifying critical functions within their divisions that are supported by technology-based information systems. The vice presidents shall decide the criticality of functions and/or assignment of responsibilities that are disputed or not organizationally apparent.

The associate vice president for information technology and CIO is responsible for identifying the technology resources that support critical functions, for developing contingency plans for critical technology-based information systems, and for representing IT within the broader continuity of operations/emergency planning context.

Development of contingency management plans for central information systems is a shared responsibility. IT is responsible for the central computing facilities and the communications network. The system owner is responsible for the contingency management plans and alternate procedures necessary to sustain functionality during the recovery period.

All departments, offices, and employees that generate, receive, or maintain public records under the terms of this policy are also responsible for compliance with Policy 1109 - Records Management.

8. SANCTIONS

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination from employment.

9. EXCLUSIONS

This policy does not refer to manual systems.

10. INTERPRETATION

Authority to interpret this policy rests with the president and is generally delegated to the associate vice president for information technology and CIO.

Previous Version: December 2020
Approved by the president: April 2002