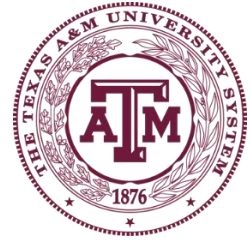


34.07.02 Business Continuity Plans

Approved September 10, 2020
Next Scheduled Review: September 10, 2025



Regulation Summary

This regulation provides the essential elements that each member of The Texas A&M University System (system) must develop in its Business Continuity Plan(s). These documents address continuity actions to be taken should the member experience a disruption of essential functions that jeopardizes operations. For the purposes of this regulation, the terms “Business Continuity Plan” (BCP) and “Continuity of Operations Plan” (COOP) are interchangeable.

Definitions

Click to view [Definitions](#).

Regulation

1. BUSINESS CONTINUITY FUNDAMENTAL ELEMENTS

Each member must establish a BCP that will be included as an annex to member emergency operations plans and must:

- (a) Determine, or establish criteria for determining, its essential functions;
- (b) Establish a continuity planning team that provides management and oversight of BCP creation and review;
- (c) Establish communication procedures related to activation and deactivation of the BCP; and
- (d) Test the annex annually, either independently or as part of a larger exercise.

2. BUSINESS CONTINUITY PLAN OR PROGRAM REQUIREMENTS

In addition to the fundamental elements referenced in Section 1, a member’s BCP must address all of the following:

- (a) Identification of decision-making authority regarding plan activation.
- (b) A set of procedures to govern orders of succession and delegations of authority.
- (c) Roles and responsibilities of key personnel during continuity operations.
- (d) Alternate facilities and/or remote work procedures:

- (1) If the use of alternate facilities is necessary, contracts/memoranda of agreement/memoranda of understanding for the use of such facilities must be obtained and included or referenced in the BCP annex. These contracts must be designated as essential records.
 - (2) If the use of remote or telework is necessary, the plan must contain procedures for the transition to remote work that addresses internet access and IT security requirements as well as remote data and software access requirements.
- (e) Procedures for the identification and procurement of resources necessary to maintain essential functions during a continuity event.
- (f) Protection of essential/vital records to include:
- (1) Procedures determining where vital records are stored and backed up, and procedures to ensure they are available for use within the required times.
 - (2) Procedures for naming and mapping vital electronic records. Existing processes can be used to fulfill this requirement if already established.

3. PLAN SUBMISSION AND REPORTING

- 3.1 Each member must submit a current copy of its BCP annex on the same time schedule as the Emergency Management Plan in accordance with System Policy *34.07.01, Emergency Management Plans*.
- 3.2 Submissions and reporting as described herein must be made through the System Office of Risk Management.
- 3.3 To the extent allowed by law, member BCPs and any associated vital records are classified as confidential information.

Related Statutes, Policies, or Requirements

[System Policy 34.07, Emergency Management](#)

[System Regulation 34.07.01, Emergency Management Plans](#)

[National Fire Protection Association \(NFPA\) 1600 – Standard on Continuity, Emergency, and Crisis Management, 2019](#)

[FEMA Continuity Guidance Circular, 2018](#)

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

System Office of Risk Management
(979) 458-6330