West Texas A&M University

The Division of Information Technology
University Information Security Standards

NIST CONTROL FAMILY
CONTINGENCY PLANNING CONTROLS

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVIEW DATE
CP-2	**Contingency Plan**	**P1**	**07/09/2017**

I. STATEMENT

West Texas A&M University is responsible for developing, distributing, coordinating, reviewing, updating, communicating, and protecting a contingency plan that includes the following items:

1. Identifies essential missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by the CIO.

II. APPLICABILITY

This Control applies to all West Texas A&M network information resources. The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

III. IMPLEMENTATION

The WTAMU contingency plan shall be distributed to key personnel and a copy stored offsite. Elements of the plan for information resources shall include:

a. Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis shall identify the following elements:

   1. Mission-Critical Information Resources (specific system resources required to perform critical functions) to include:
      A. Internal and external points of contact for personnel that provide or receive data or support interconnected systems.

      B. Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.

   2. Disruption impacts and allowable outage times to include:
      A. Effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.
      B. Effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes.

   3. Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:
      A. Preventive controls and processes such as backup power, excess capacity, environmental sensors and alarms.

      B. Recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.

b. Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.

c. Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan.

d. Disaster Recovery Plan--Each state organization shall maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan.

   The disaster recovery plan will:

   1. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;

   2. Identify recovery resources and a source for each;
   3. Contain step-by-step implementation instructions;
   4. Include provisions for annual testing.