<<Prev Rule

Texas Administrative Code

Next Rule>>

TITLE 1	ADMINISTRATION
PART 10	DEPARTMENT OF INFORMATION RESOURCES
CHAPTER 202	INFORMATION SECURITY STANDARDS
SUBCHAPTER B	SECURITY STANDARDS FOR STATE AGENCIES
RULE §202.24	**Business Continuity Planning**

(a) Business Continuity Planning covers all business functions of a state agency. It is a business management responsibility. State agencies shall maintain written Business Continuity Plans that address information resources so that the effects of a disaster will be minimized, and the state agency will be able either to maintain or quickly resume mission-critical functions. The state agency head or his or her designated representative(s) shall approve the plan. The plan shall be distributed to key personnel and a copy stored offsite. Elements of the plan for information resources shall include:

(1) 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:

(A) Mission Critical Information Resources (specific system resources required to perform critical functions) to include:

(i) Internal and external points of contact for personnel that provide or receive data or support interconnected systems.

(ii) Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.

(B) Disruption impacts and allowable outage times to include:

(i) 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.

(ii) Effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes.

(C) Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:

(i) Preventive controls and processes such as backup power, excess capacity, environmental sensors and alarms.

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

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

(3) Implementation, testing, and maintenance management program addressing the initial and ongoing

testing and maintenance activities of the plan.

(4) Disaster Recovery Plan--Each state agency 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:

(A) Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;

(B) Identify recovery resources and a source for each;

(C) Contain step-by-step implementation instructions ;

(D) Include provisions for annual testing.

(b) Mission critical information shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized state agency representatives.

Source Note: The provisions of this §202.24 adopted to be effective November 28, 2004, 29 TexReg 10703; amended to be effective September 17, 2009, 34 TexReg 6315

Next Page Previous Page

List of Titles | Back to List

HOME | TEXAS REGISTER | TEXAS ADMINISTRATIVE CODE | OPEN MEETINGS | HELP |