



BEST PRACTICE

Technology Disaster Recovery Planning (1999 and 2007) (CAAFR)

Background. Governments provide many essential services to their citizens. The disruption of these services following a disaster could result in significant harm or inconvenience to those whom a government serves. State and local governments have a duty to ensure that disruptions in the provision of essential services are minimized following a disaster. Today the public sector, like the private sector, relies heavily upon computers and other advanced technologies to conduct its operations. Therefore, disaster recovery planning, in order to be effective, must specifically address policies and procedures for minimizing the disruption of government operations if computers or other advanced technologies are disabled following a disaster.

Recommendation. The Government Finance Officers Association (GFOA) recommends that every government formally establish written policies and procedures for minimizing disruptions resulting from failures in computers or other advanced technologies following a disaster. These written policies and procedures should be evaluated annually and updated periodically, no less than once every three years.

At a minimum, a government's policies and procedures for computer disaster recovery should do all of the following:

- *Formally assign disaster recovery coordinators for each agency or department to form a disaster recovery team.* The responsibilities of team members should be defined and a current list of team members and their telephone numbers should be maintained. The government should also establish procedures for assembling the team in the event of a disaster.
- *Require the creation and preservation of back-up data.* A government's procedures in this regard should cover the regular and timely back-up of computer data (with proper documentation) and the transportation and storage of back-up data off-site (with proper documentation). The government should also ensure the security of back-up data both during transport off site and during storage off site.
- *Make provisions for the alternative processing of data following a disaster.* A government should enter into a contract for the alternative processing of data following a disaster. It is essential that the government carefully monitor software upgrades to ensure that any such alternative processing site remains capable of processing the government's data. A government should also establish processing priorities should the use of the alternative processing site become necessary. In addition, in situations qualifying for federal emergency assistance, it is essential that the government be capable of providing information to the federal government in the format mandated by the Federal Emergency Management Agency.
- *Provide detailed instructions for restoring disk files.*
- *Establish guidelines for the immediate aftermath of a disaster.* Specifically, the government's computer disaster recovery plan should provide guidelines for declaring a disaster, for issuing press releases and dealing with the media, for recovering communications networks, and for assessing damage –

- A copy of the government's formal computer disaster recovery policies and procedures should be kept off-site to ensure its availability in the event of a disaster;
- Every government should annually test its computer disaster recovery plan, including communication within the disaster recovery team, and take immediate action to remedy deficiencies identified by that testing. It is essential that such testing encompass the restoration as well as the processing of the government's data; and
- A government also should satisfy itself concerning the adequacy of disaster recovery plans for outsourced services.

Approved by the GFOA's Executive Board, March 2, 2007.