STATE OF ALABAMA

Information Technology Policy

POLICY 673-00: BACKUP AND RECOVERY

An important information system design and operational consideration is the ability to recover and restore data/information, should a problem occur. An integral part of ensuring security and integrity of the computing and network environment, and the availability of data, is a well-structured, documented, and tested backup and recovery program.

OBJECTIVE:

Establish responsibilities for backup and recovery of State of Alabama computing resources.

Establish requirements for backup and recovery of State of Alabama computing resources.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

Ensure information system security plans include back-up and recovery procedures. As a minimum, backup and recovery procedures shall provide the following:

- System configuration and hardware component descriptions
- Recovery prioritization
- Tested procedures for restoring the system
- Tested procedures for restoring and testing applications
- Tested procedures for restoring and verifying data from backup sources

For mission-critical systems, store backup copies of the operating system and other critical information system software in a separate facility or in fire-rated containers that are not collocated with the operational software.

Identify alternate storage sites and initiate necessary agreements to permit the storage and timely and effective recovery of information system backup information (alternate storage sites should be sufficiently geographically separated from the primary storage site so as not to be susceptible to the same hazards).

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) shall be based on the application, system, or data owner's recovery time and recovery point objectives.

Ensure service providers, vendors, and other third parties who store software or data used in conducting State of Alabama business provide evidence of full compliance with applicable State standards upon request of the application, system, or data owner, Network Operations Group, or IT Manager.

Application, System, and Data Owners:

Ensure that production software and data are appropriately backed up in compliance with applicable State standards.

Provide detailed backup and recovery requirements to the respective Network Operations Group and/or System Administrators.

Maintain written procedures and documentation on the backup and recovery of software and data.

Conduct proper backup and recovery due diligence when contracting with service providers, vendors and other third parties.

System Administrators and/or IT Managers:

Conduct backups of user-level and system-level information (including system state information) contained in the information system in accordance with data owner specifications and system security plans, and store backup information at an appropriately secured location.

- Provide the tools, methodology, and schedules required to backup and recover application software, data, and network device configurations on State of Alabama networks.
- Maintain written procedures and documentation related to the backup and recovery process.

Employ mechanisms with documented supporting procedures to allow the information system to be recovered and reconstituted to its original state after a disruption or failure (Note: “original state” means all system parameters, either default or organization-established, are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available, and the system is fully tested).

Include a full recovery and reconstitution of the information system as part of contingency plan testing.

Test back-up and recovery procedures at least twice annually.

Selectively use backup information in the restoration of information system functions as part of contingency plan testing.

Information System Users:

Users are responsible for saving data to locations that afford proper back up and recovery.

.

ADDITIONAL INFORMATION:

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
673-00	09/01/2011	Combines and replaces Policy 670-07 and Standard 670-07S1