# STATE OF ALABAMA

## Information Technology Policy

# POLICY 678-00: SYSTEM MAINTENANCE

Information systems must have security controls in place to protect the routine maintenance activities that enable the system to function correctly. Routine maintenance activities include diagnosing and correcting hardware, firmware, and software problems; loading, maintaining, and updating software, device drivers, configuration settings, etc., and maintaining a historical record of system changes. Such activities may be conducted in-house or by individuals communicating through an external, non-organization-controlled network (e.g., the Internet) further exposing systems to attack.

### OBJECTIVE:

Ensure all maintenance, diagnostic, and repair activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location, are managed and monitored to preserve the confidentiality, integrity, and availability of State information system 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:

Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

- Explicitly approve the removal of information system or system components from organizational facilities for off-site maintenance or repairs.
- Following maintenance or repair actions check all potentially impacted security controls to verify that the controls are still functioning properly.

Control and monitor the use of information system maintenance tools.

- Inspect all maintenance tools brought into a facility by maintenance personnel for obvious improper modifications.
- Check all diagnostic and test program media for malicious code before use.
- Document approved maintenance tools in system operating procedures.

Authorize and control non-local maintenance and diagnostic activities.

- Log all non-local maintenance, diagnostic, and service activities. Maintenance logs should be reviewed daily, but shall be reviewed at least weekly.
- Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions. Whenever possible, utilize two-factor authentication on remote maintenance ports.
- Ensure that remote maintenance port access is normally blocked unless unattended access is required. Whenever possible, require some involvement of local personnel in opening remote maintenance ports.
- Whenever possible, turn off maintenance features when not needed.
- Keep maintenance terminals in locked, limited-access areas.

- When maintenance is completed terminate all sessions and remote connections. If password-based authentication was used during remote maintenance, change the passwords following each non-local maintenance service.

Allow only authorized personnel to perform maintenance on State information systems.

- Maintain a list of authorized maintenance personnel including third-party maintenance providers.
- When maintenance personnel do not have the needed access authorizations, organizational personnel with appropriate access authorizations and sufficient technical competence shall supervise maintenance personnel during the performance of information system maintenance activities.

## ADDITIONAL REQUIREMENTS:

The following additional requirements, based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-53: *Recommended Security Controls for Federal Information Systems and Organizations*; shall be applied to information systems which if unavailable would cause a moderate to severe impact to organizational productivity or services.

### MAINTENANCE RECORDS:

Maintain information system maintenance records for the life of the system that include:

- Date and time of maintenance
- Name(s) of the individual(s) performing the maintenance
- Name of escort (if necessary)
- Description of maintenance performed
- List of equipment removed or replaced (including identification numbers if applicable)

### THIRD-PARTY MAINTENANCE PERSONNEL:

Third-party maintenance providers under contract to perform maintenance/support services on State information systems shall provide a list of field service engineers assigned to support State maintenance contract with the following information for each service representative:

- Name
- Company represented
- Title
- Contact Info (phone number; e-mail)
- Photo for identification purposes
- List of systems individual is authorized to perform maintenance on

### TIMELY MAINTENANCE OF SECURITY-CRITICAL COMPONENTS:

Specify the security-critical information system components that, when not operational, result in increased risk to the organization, individuals, or the State because the security functionality intended by that component is not being provided. Security-critical components may include, for example, firewalls, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.

Conduct a risk assessment and analysis/determination of need for the continuity of operations of security-critical information system components to determine the maximum tolerable downtime duration.

Ensure maintenance support and spare parts for the identified list of security-critical information system components is obtained within the defined time period.

Document maintenance requirements in operational procedures.

## SUPPORTING DOCUMENTS:

- Information Technology Policy 623: Authentication
- Information Technology Standard 622S2: Dial-In Access/Modem Use

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

## DOCUMENT HISTORY:

| Version | Release Date | Comments |
|---|---|---|
| 678-00 | 09/01/2011 | Replaces Policy 670-08 and Standard 670-08S1 (both are hereby rescinded) |
| | | |
| | | |