

STATE OF ALABAMA

Information Technology Policy

POLICY 621-01: NETWORK AND SYSTEMS ACCESS

Access to State of Alabama networks and information systems must be authorized, authenticated, and audited to ensure that only authorized users gain access to State networks, systems, applications, and data. This policy defines account management requirements and responsibilities to include access authorization, audit, termination, and enforcement.

OBJECTIVE:

Manage the granting and rescinding of access to State of Alabama networks and information systems, plan and utilize appropriate access enforcement mechanisms, and ensure user accountability.

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:

Manage (establish, activate, modify, review, disable, and remove when no longer needed) information system and network access accounts. To ensure individual accountability, every State network and/or information system user shall have an individual network and/or system access account (i.e., a unique user identifier).

Advise information system users that authorized access does not imply a right to privacy. Advise users that system and network activities may be monitored, recorded, and are subject to audit by management or other authorized personnel.

Management or authorized personnel shall review audit records (e.g., user activity logs) for inappropriate activities and compliance with State and agency policies and standards. Investigate any unusual information system-related activities and periodically review changes to access authorizations.

ADDITIONAL REQUIREMENTS:

The following requirements are 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 other best practices.

Access Authorization:

System and Network Administrators shall:

- Ensure that all requests to establish access accounts are approved by a designated manager, supervisor, or the system owner.
- Maintain a record of all users authorized to access the system identifying the user name and unique user ID, level of authority granted, user location, the date access was granted, and the date access will terminate (or was terminated).
- Monitor and review the granting and rescinding of network and system access.

Temporary Access:

Temporary access may be granted if required for service providers (contractors, vendors, and business partners) or external regulators.

All requests for temporary access shall be made in writing and shall be subject to management or system owner approval.

Temporary access shall be valid only for a specified period of time and shall be disabled immediately upon expiration or when no longer required, whichever occurs first.

Short-term (less than one day) access to the State network without identification or authentication shall be limited to Internet access and connections to other publicly available information systems. Access points providing unauthenticated access shall be closely monitored and, when practical, shall be disabled if/when not needed.

Access Termination:

Managers/Supervisors shall:

- Notify applicable System Administrator(s) in writing within 48 hours of an employee termination, start of long-term (greater than 30 days) leave, or a contract person completing their assignment. If termination is for cause, notification shall be made immediately upon or prior to termination action.
- Advise administrators of actions regarding disposition or preservation of user files and accounts.

Network and System Administrators shall:

- Disable access to networks, application systems, and data when advised by management.
- Ensure the user account(s) and all system access is disabled/revoked immediately when a user separates from an organization (regardless of reason).
- Ensure user accounts are reviewed periodically and inactive accounts are handled as follows:
 - User accounts that have been inactive for more than 60 days shall be disabled or revoked.
 - User accounts that have been inactive for more than 6 months shall be deleted.

Access Enforcement:

Access to all State information is determined by both its protection category and user need-to-know. Need-to-know shall be determined by the information owner and enforced by appropriate access controls.

Access Enforcement Mechanisms:

Employ access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in State information systems.

Employ access enforcement mechanisms at the application level, when necessary, to provide increased information security.

If encryption of stored information is employed as an access enforcement mechanism, ensure the cryptography used is compliant with FIPS 140-02 (as amended) and State IT policy.

Ensure that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).

Separation of Duties and Least Privilege:

Information systems shall enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions.

ADDITIONAL INFORMATION:

Information Technology Policy 683: Encryption

http://cybersecurity.alabama.gov/documents/Policy_683_Encryption.pdf

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
621-00	09/01/2011	Replaces Policy 620-01 and Standard 620-01S1
621-01	11/23/2011	Modified access termination (revocation and deletion) requirements