# STATE OF ALABAMA

## Information Technology Guideline

# GUIDELINE 606G2-00: PERSONNEL SECURITY

Personnel Security refers to the practices, technologies, and/or services used to ensure that personnel security safeguards are applied to the access and use of information technology resources and data. Such safeguards include (but are not limited to):

- Granting or withdrawing physical and system access privileges based on the principles of need-to-know and least privilege
- Training personnel on security policies, procedures, and best practices (commensurate to one's duties and responsibilities)
- Executing Non-Disclosure Agreements for individuals needing access to sensitive or confidential information (prior to granting access to that information)
- Conducting personnel screening and background checks (when required by organizational policy)

Personnel security controls (such as those listed above) are intended to reduce the risk of compromise of key information technology assets (information systems and data).

### OBJECTIVE:

Ensure personnel security controls and related procedures are implemented to protect the privacy, security, and integrity of information technology resources against unauthorized or improper use.

### SCOPE:

The guidelines in this document apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

### GUIDELINES:

Personnel security should be an integral part of an organization's IT security plan. Organizational management needs to ensure that safeguards are implemented to protect information systems and data from adverse impact caused by the actions of individuals by ensuring an appropriate level of trust.

Managers can balance the concern for the safeguard of information system resources with the personal integrity of organizational personnel by implementing the practices described in this guideline. Managers and Supervisors should coordinate with Human Resources and IT Department personnel to facilitate these practices.

## PERSONNEL SECURITY POLICY AND PROCEDURES

Organizations should develop, disseminate, and review/update (annually or at organization-defined frequency) formal, documented personnel security policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with the following recommended safeguards pertaining to personnel security.

Personnel security procedures can be developed for the security program in general and for a particular information system, when required.

Organizational risk management strategy should be a key factor in the development of the personnel security policy.

## POSITION CATEGORIZATION

Management should define all positions within the organization.

In defining IT-related positions two general principles should be followed: *Separation of Duties* and *Least Privilege*. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. Least privilege refers to granting a user only those accesses they need to perform their official duties.

Information system access controls should further enforce these principles (as required by State IT Policy 621).

Organizational Management should:

- Assign a risk designation to all positions (for example: designate every position within the organization at a high, moderate, or low risk level as determined by the position's potential for adverse impact to the efficiency and integrity of a service, an information system, or of the corresponding data)
- Review position risk designations at least once every three years and revise as needed
- Establish screening criteria for each position (see Personnel Screening, next section)

## PERSONNEL SCREENING

Testing and background screening should be used as appropriate to help determine or validate a candidate's qualifications, past performance and appropriateness for a particular position.

Organizations should consider background screening for candidates or employees whose job responsibilities require that they have elevated system user privileges or access to sensitive and confidential information.

Organizations should define the conditions where initial screening in required, conditions requiring re-screening, and the frequency of such re-screening.

Initial screening (when required) should be conducted prior to authorizing access to information systems or data.

## PERSONNEL TERMINATION AND TRANSFER

Employee access to all systems and information must be removed concurrent with when the requirement for access no longer exists (e.g., as result of termination, transfer, or change of duties).

Required actions pertaining to network and information systems access resulting from personnel termination or transfer are described in State IT Policy 621: Network and System Access.

It is the responsibility of the supervisor to initiate the required actions based on the circumstances.

## THIRD-PARTY PERSONNEL SECURITY

Organizations should establish personnel security requirements, including security roles and responsibilities, for third-party providers. This includes, for example, contractors and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

Organizations should:

- Document all third-party personnel security requirements
- Monitor provider compliance
- Explicitly include personnel security requirements in acquisition-related documents

Additional information security requirements for service providers are documented in State IT Policy 602: Information Security for Service Providers.

## ADDITIONAL INFORMATION:

Information Technology Policy 602: Information Security for Service Providers
http://cybersecurity.alabama.gov/documents/Policy_602_Info_Security_for_Service_Providers.pdf

Information Technology Policy 606: Risk Management
http://cybersecurity.alabama.gov/documents/Policy_606_Risk_Management.pdf

Information Technology Policy 621: Network and System Access
http://cybersecurity.alabama.gov/documents/Policy_621_Network_System_Access.pdf

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

*By Authority of the Office of IT Planning, Standards, and Compliance*

## DOCUMENT HISTORY:

| Version | Release Date | Comments |
|---|---|---|
| 606G2-00 | 01/18/2012 | Original document |
| | | |
| | | |