	Georgia Technology Authority	
Title:	**Personnel Security**	
PSG Number:	**PS-08-014**	
Effective Date:	03/20/2008	**Review Date:** 09/15/2024
Synopsis:	Requirements for identity verification of IT employees and contractors	

PURPOSE

In support of the Department of Homeland Security's initiatives to mitigate the risks of identity fraud, counterfeiting, and terrorist exploitation among personnel entrusted with physical and logical access to state government facilities and information resources, it is essential that the State establish a requirement for identification verification for all state personnel and engagement contractors.

Additionally, personnel security is essential to establishing a common baseline of trust between state agencies in support of statewide data-sharing requirements.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(10) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(21) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Policy*

TERMS AND DEFINITIONS

Federal work authorization program - any of the electronic verification of work authorization programs operated by the US Department of Homeland Security (USDHS) or any equivalent federal work authorization program operated by the USDHS to verify information of newly hired employees.

POLICY

Each state agency shall:

- Verify the identity, employment eligibility and conduct background screenings for all state employees and engagement contractors through a Federal Work Authorization Program in accordance with O.C.G.A §§ 13-10-91 before granting access credentials to State of Georgia facilities or information resources not designated as public access resources.

- Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) meet established security and qualification criteria for those positions.
- Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and/or transfers.
- Ensure that individuals are aware of all information security policies and procedures, their responsibilities and the consequences for failing to comply.
- Employ formal sanctions for personnel failing to comply with security policies and procedures.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Personnel Identity Verification and Screening (SS-08-017)
Third-Party Security Requirements (SS-08-011)

REFERENCES

Rules of Georgia Department of Labor, Chapter 300-10-1 “Georgia Security and Immigration Compliance Act of 2006”

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations