	Georgia Technology Authority	
Title:	**Authorization and Access Management**	
PSG Number:	**SS-08-010.02**	
Effective Date:	12/15/2014	**Review Date: 12/29/2023**
Synopsis:	Requires managed access to state facilities and information resources	

PURPOSE

Lack of managed access controls to sensitive or proprietary state information assets can result in unauthorized or inadvertent disclosure, modification or deletion of the information asset or render it unavailable. Access Control measures are needed to ensure that even legitimate users have access to only the information for which they are authorized and need to perform their official duties. This standard establishes minimum access control requirements.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(8) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(20) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Charter*

TERMS AND DEFINITIONS

Access Control - the set of rules and deployment mechanisms that enable or restrict physical and logical access to information systems.

Physical Access - the ability to enter areas or facilities where information systems and technology assets reside.

Logical Access - the ability to read, write or, execute records or data contained in the information system.

Identity and Access Management - a set of processes and supporting infrastructure for creating, maintaining, and using digital identities in accordance with business policies and needs.

Authorization - the formal approval, granted by Data Owner, for an individual to gain access to a facility, system, or other non-public information asset.

Data/Information Owner - a business person who defines the controls necessary to protect the data within their business function and accepts the risks associated with operating an information system processing that data.

System Owner - the individual responsible for system operations and authorizes access to system-level or administrative functions.

Positive User Identification - the validation of user requesting and being granted access credentials to non-public state information resources.

Access Privileges or Rights - refers to powers granted to a system user that defines the levels of access they have to read, write, or execute data or system resources.

Need-to-Know - a confidentiality principle that says access should be denied even if an individual has all the necessary official approvals to access certain information but does not need access to the specific information to conduct one's official duties

Principle of Least Privilege - refers to assigning access rights that provide the most restrictive access or provides no more access to systems or information than is necessary to perform one’s official duties.

User Provisioning - refers to the creation, maintenance and deactivation of user objects and user attributes.

Public Access Information/System - refers to any information asset (usually a public web-facing application) that is designated for use by and available to the general public with or without user authentication.

STANDARD

Agencies that create, use or maintain information assets of the State of Georgia shall implement access control measures that restrict physical and logical access to information, information systems and facilities to only authorized individuals, except where specifically designated as public access resources.

Access to state information resources, not designated for general public use, shall require a formal process of identity and access management to include positive user identification, explicit Data Owner approval, user provisioning, and system authentication.

Data Owner or designee shall establish and document access authorization and management policies and procedures that clearly define request and approval processes for granting, modifying, revoking and monitoring access to the information assets.

System Owners shall develop formal processes for identity and access management and issue and manage access credentials in accordance with Data Owner policy and procedures.

System Owners shall establish and document procedures governing access authorization and management of Privileged Users (super-users, developers, testers, system administrators and/or system/service accounts for auto processing).

Privileged access activities on systems categorized as moderate or high shall be audited.

Access credentials shall be granted based on the principle of least privilege, need-to-know, specific business needs and job function.

Privileged Users shall not use their super-user credentials to perform non-system related functions or to access system for which they do not need such access such as but not limited to HR and personal business matters.

Developer access to production environments shall be prohibited or limited and all activity audited and monitored.

Access credentials for production environments shall be different from those of development/test environments.

Misuse of privileged access shall be reported in accordance with established agency incident response and reporting procedures.

Access granted to third parties (contractors/consultants etc.) requires a signed contract and should be terminated when the contract is completed or earlier if the access is no longer required.

Access privileges shall be terminated or modified promptly upon a change in duties, employment status or extended periods of inactivity.

Access to state information resources granted to the general public (i.e. public web applications), shall be physically or logically segregated from all non-public (state proprietary) resources in specially designated public domain resource configurations.

Default access privileges shall be set to “deny all” or “no access” Information Security Officers, Data Owners or their designee shall conduct periodic reviews of access control lists and logs to validate the appropriateness of user accounts and use of access privileges.

REFERENCES

Georgia Open Records Act
Georgia Computer Crimes Act
NIST Computer Security Resource Center - **http://csrc.nist.gov/** SP 800-53 Recommended Security Controls

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Access Control (PS-08-009)
Password Authentication (PS-08-006) Third-Party Access (PS-08-011)
Network Access-Session Controls (SS-08-048)
Information Security Management Organization (SS-08-006)