
Topics:

[access](#) [2], [data owner](#) [3], [employee](#) [4], **[Authorization and Access Management](#) [1]**

SS-08-010.02 Authorization and Access Management

Issue Date: 3/31/2008

Effective Date: 12/15/2014

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 that information for which they are authorized and need to perform their official duties. This standard establishes minimum access control requirements.

SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS

Enterprise Information Security Charter [PS-08-005](#) [5]

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 that of development/test environments.