Procedures for Certification of Security Access for OSC Enterprise Application Systems

Pursuant to the Office of the State Controller's (OSC) Policy and State Security Standard SCIO-SEC-301-00, Access Control Policy, Section AC-2, Account Management, requirement "v," each state entity that uses an OSC enterprise application system shall:

1) Monitor the use of information system accounts, and
2) Review accounts for compliance with account management requirements at least annually for user accounts and semi-annually for privileged accounts/roles.

Privileged accounts are accounts with elevated access and/or agency-defined roles that allow those individuals to perform certain functions that ordinary users of that system are not authorized to perform. These privileged roles may include, for example, root access, system administrator access, key management, account management, network and system administration, database administration, and website or server administration.

Responsibilities

Management of each state entity using an OSC enterprise application system is responsible for assigning the access rights for each of their employees requiring system access. It is management's responsibility to ensure compliance with all applicable internal control standards (i.e., segregation of duties – each user profile should be reviewed to ensure the access rights are compatible with the user's job functions).

Management is responsible for ensuring that proper controls, policies, and procedures to prevent, detect, and correct abuse of the OSC enterprise application system security privileges have been designed and are in place.

Management is responsible for promptly notifying OSC of any problems, violations, or changes with a user's access rights. Timely notification is essential when a user changes job functions and/or leaves the entity.

All OSC enterprise application systems users are responsible for reading and complying with all applicable OSC policies and procedures governing the specific application accessed by the user.

Procedures

On an annual basis and on a semi-annual for all privileged accounts, the Chief Financial Officer (CFO) of each state entity shall review report(s) of all users of OSC's enterprise application systems to determine:

1) If all users listed are still active employees, and

2) If the access rights for all listed users remain compatible with their job functions.

Reports for each OSC enterprise application system are available at:

https://files.nc.gov/ncosc/documents/Policies/ReportsForCertificationOfSecurityAccessForOSCEnterpriseApplicationSystem%2801132016%29.pdf

Each state entity shall promptly notify OSC Support Services of any required changes by submitting an OSC Application Systems User Access Rights Change Form for each affected user.

Documentation that supports the state entity's review should be maintained in accordance with OSC policy requirements.

The Certification of Security Access form is available from the OSC website under the Certification of Security Access link at:

https://files.nc.gov/ncosc/documents/Policies/Form_for_Certification_of_Security_Access_for_OSC_Enterprise_Application_Systems.pdf

This form is used to certify compliance with OSC policy requirements pertaining to the review of user access rights for OSC's enterprise application systems and is to be completed by the entity's Chief Financial Officer and Internal Control Officer. This form and supporting documentation shall be maintained by the state entity as prescribed in the policy and on the form.