
Technology Standard

Assignment of the *Super User* Security Role

Version: 1.1

Status: *Approved: 04/16/08*

Contact: *Director, Technology Administration Services*

PURPOSE

The VCCS provides shared information technology resources and services to faculty, students, staff, and college patrons for activities supporting the VCCS mission. The purpose of this standard is to protect the integrity of VCCS Technology Resources and the users thereof against unauthorized or improper use of those resources. All individuals (VCCS and otherwise) granted access to this security role will be required to follow the guidance documented in this standard.

SCOPE

The following standard describes the responsible use expected by those given access to the technology resources and services supporting the VCCS Student Information System (SIS) and Administrative Information System (AIS). The standard defines the Super User security role and establishes the specific requirements governing the assignment and use.

APPLICABILITY

This standard is applicable to the System Office and all colleges.

DEFINITION

As a part of the AIS and SIS security model VCCS provides a special set of permissions, often described as the "Super User" role, which has access to all panels (navigations) available in the system except those supporting security administration and the "Enrollment" panel. The role as defined also permits those who are assigned this role full authority to read, change, and delete the information stored in the associated databases.

STANDARD

In accordance with COV SEC501-01 standard and the VCCS Personnel Security standard the principle of **least privilege** must be used by each college and the System Office in the assignment of security roles and responsibilities. Faculty, staff, administrators, and other users requiring access to enterprise systems should be granted only those privileges necessary to perform their normal work duties as documented in their employee work profile or other formal documents that detail job duties. Therefore given the current authority and scope of access assigned to the *Super User* security role and other similar privileged security roles access must be strictly limited to those personnel as determined by the needs of the colleges and System Office. However the following must apply:

1. All System Office and college assignments in the production instance (except VCCS security administrators) must be reviewed and authorized every 120 days. The account will be automatically deleted if a renewal is not approved.
2. All requests should be fully documented outlining the need and specific work to be accomplished.
3. Request for access to the production instance must be authorized by the immediate supervisor, agency head or their designee, the data owner, and system owner.
4. The entity (college or System Office) who grants an individual the *Super User* role is responsible for ensuring that the individual(s) assigned to this role has all the required knowledge, training, and related skill sets necessary to effectively perform the work under the *Super User* security role.
5. The entity (college or System Office) that submits the request for an individual to be assigned the Super User security role is ultimately responsible for the work performed under this privileged account. Therefore they are expected to implement internal procedures and/or processes that ascertain that the use of the "Super User" role is appropriate and can be substantiated as required.

6. The entity (college or System Office) information security officer must maintain a file of all requests and written and/or electronic documentation for *Super User* for periodic review by the Internal Audit Office and VCCS Security Office. These records shall be stored and safeguarded in a manner consistent with all applicable record retention policies and guidelines and made available upon request.

7. Any exceptions to this standard must be fully documented by the entity (college or System Office) and the information forwarded to the System Office for verification and review.

Access methods, like the *Super User*, are at risk for potential abuse primarily through well-intentioned misuse. In the extreme, changes to the production application and database using the *Super User* can leave elements of the database in an error state, and the validity and integrity of student and institution data could be compromised. This standard proposes a set of practical procedures for safeguarding the VCCS IT enterprise applications and data.

Note: The role of System Owner is temporarily delegated to the college president or their designee.