



Personnel Security Standard

Personnel Security

Version: 1.0

Status: Approved: 04/16/08

Contact: [Director, Technology Administration Services](#)

PURPOSE

This standard is intended to ensure security controls and related procedures are implemented to protect the privacy, security and integrity of VCCS information technology resources against unauthorized or improper use, and to prevent and detect attempts to compromise information technology resources for any employee who is separated, transferred, or promoted.

SCOPE

In accordance with the Commonwealth of Virginia (COV) Information Technology Resource Management Standard (ITRM), [COV ITRM Standard SEC501-01](#), Information Technology Security, personnel security must be an integral part of a VCCS information technology security

Personnel Security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied. Personnel security safeguards take into account 1) granting or withdrawing physical and system access privileges upon: hiring an employee, transferring an employee to another VCCS Entity or state Agency, terminating an employee, or when an employee resigns or changes job duties within a VCCS Entity; 2) system access will be granted, modified and revoked via a formal and auditable process, 3) security training to reinforce this standard will be conducted within 30 days of a new hire, 4) Non-Disclosure Agreements will be signed by all individuals who need access to "sensitive/confidential" information, prior to granting access to that information, 5) Background checks of personnel may be required consistent with VCCS Entity policy and depending on the sensitivity/confidentiality of information accessible to that position.

Auditable Process refers to specific documentation which can be a manual or an automated process that provides sufficient evidence that will allow one to trace the events of an action that has taken place.

Sensitive Data/Information refers to critical information for which the unauthorized access, loss, misuse, modification, or improper disclosure could negatively impact the ability of the VCCS Entity to provide services and benefits to its students.

Confidential Data/Information refers to information that involves the privacy to which individuals are entitled by law. This information may only be disclosed to those individuals that are authorized and have a need to review the data or information.

STANDARD

Personnel security begins during the staffing process. Best practices suggest that two general principles should be followed in defining a position: *separation of duties* and *least privilege*.

Separation of duties (SoD) is an important concept in developing the required internal controls for an organization. As a security principle, it has as its primary objective the prevention of fraud and errors. Separation of duties refers to dividing roles and responsibi

individual with access to critical system security controls; i.e., controlling who is allowed to enable or disable system security features or change the privileges of users or programs. Best practice suggests it is better to have several administrators with limited access to security resources rather than one person with "super user" permissions.

Least Privileges requires that each user account in a system be granted the most restrictive set of privileges needed to perform authorized tasks. Ensuring least privilege requires identifying what responsibilities are, determining the minimum set of privileges to perform the job,

The System Office and all colleges must establish and document the process which directs the steps and the timing required to grant and withdraw physical and system access privileges to personnel for the following events: new hire, employee transfer to another VCCS office or location, employee separation, employee resignation, employee change of job duties, and documented disgruntled employee behavior. See related links below for additional guidance.

RELATED LINKS

[Access Control and Determination](#)
[IT Security Awareness Training](#)
[Acceptable Use](#)



[Return to Standards](#)