Access Management Control

Version	Date	Framework References	Informative References	Approver/s
1.0		PR.AC-1 PR.PT-3	PCI 7.1 CCS CSC 16 CCS CSC 6	Security Workforce Action Team

Introduction

Without defined access privileges and control, users would be allowed to access systems and applications in CCRI's data environment, and be able to view, delete, and tamper with stored data, code, and configurations. Therefore, controlling who has access to what and what actions they are permitted to perform is important to support systems and applications transmitting, processing, and/or storing sensitive data from unauthorized access. CCRI's data environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of data.

A careful review of each system and application should be performed based on results from risk assessment activities performed by each functional area, and user's granted access privileges based upon the principle of "business need-to-know" (where access is based on whether the individual requires access based upon their function or role). The general rule to follow is that all users start with no access privileges and are granted access to systems, applications, tools, etc. individually, as needed. All access granted is to be tracked by the system/ application administrator within the functional area or centralized in the active directory by IT depending on the specific application or system, and reviewed on a semi-annual basis as users may leave the company, temporarily need access to specific systems, or change positions whereby they no longer require access privileges. See addendum A Access Management Administrator List.

Access to critical systems, applications, equipment, and data is required in order for CCRI to maintain business operations; however any user possessing privileges they do not require can lead to an intentional or unintentional security breach, causing harm to CCRI's finances, operations, and brand name.

Purpose

This Access Management Control details the requirements for the granting, transferring, revoking and management of user access in CCRI's data environment.

Scope

This control applies to CCRI employees, student employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at CCRI, whether conducting activities on CCRI premises or off-site. Student access to systems should be especially limited in nature and necessity clearly defined.

General Student Access

Students may access their MyCCRI account which includes information about themselves and necessary tools to complete academic and administrative functions such as registering themselves, email, print services, or paying their bill.

When a student takes on additional roles in the college, such as becoming a student employee, a separate user ID is to be created for that role and access will be strictly limited to performing that role.

Students are to acknowledge CCRI's acceptable use policy when creating a student account.

To reduce impediments for returning students, accounts are allowed to remain active as long as technically feasible.

This control applies to all systems, applications, and equipment owned or leased by CCRI whether located on CCRI premise or off-site, and all CCRI locations where CCRI data is present.

Distribution

This control is to be distributed to all those with responsibilities for maintenance and management of networking equipment at CCRI, to include CCRI employees, student employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

Exceptions

There are no exceptions to this policy.

Violations

Individuals found to have violated this control may be subject to disciplinary action and possible termination of employment.

Review Schedule

This control will be reviewed on an annual basis by the CCRI Security Workforce Action Team.

Control

Access Privileges

Users are to be assigned access privileges based upon the individual's business role and function, following the practice of business need-to-know and right-to-know. A structure of role based access control should be established so that specific functions receive standardized levels of access. Once assigned, the access granted should be reviewed to ensure that it is the lowest level necessary for the user to perform their job requirements.

Acknowledgement of Access

Users are to receive CCRI's information security control and sign their acknowledgement of following CCRI's requirements prior to gaining access.

Tracking

All access granted, transferred, or revoked is to be tracked in an approved CCRI access tracking mechanism, and signed by the user's manager and the system owner prior to being granted. This form should include the user's name, location, department, date of access action taken, model after existing user (if applicable), and the access granted.

Review

Access privileges are to be reviewed on a semi-annual basis by the user's manager and the system owner.

Inactive or Disabled Accounts

Access accounts found to be inactive or not appropriately assigned are to be disabled/revoked and removed within 90 days for PCI/high risk systems and 365 days for low to moderate risk systems.

Granting Access

The user's manager and the system owner are to approve the access prior to it being granted.

Changing Access

The user's manager and the system owner are to approve the access prior to it being changed.

Removing Access

If the user has been terminated from the college, the user's manager must notify the system owner to disable/revoke the user's access by a specific date or immediately. If the user holds privileged access to

PCI systems or high risk data, their access ID should be removed unless it is absolutely critical for business operations. Low to moderate risk systems may remain active up to one year for workers that are employed on an academic period basis.