Information Systems Access Policy

Overview

Managing access to UACCM information systems is paramount to maintaining the security and integrity of the information stored on these systems.

Purpose

The purpose of this policy is to maintain an adequate level of security to protect UACCM data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of UACCM information systems.

1. Policy

1.1 Access

1.1.1 Only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

1.1.2 Who is Affected: This policy affects all students and employees, and all contractors, consultants, temporary employees and business partners. User who deliberately violate this policy will be subject disciplinary action.

1.1.3 Affected Systems: This policy applies to all computer and communication systems owned or operated by UACCM and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

1.1.4 Entity Authentication: Users (remote or internal), accessing UACCM networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- Unique user identifier
- At least one of the following:
    - Biometric identification
    - Password
    - Personal identification number
    - A telephone callback procedure
    - Token

1.1.5 Third Party Access: Individuals who are not students, employees, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use the UACCM computers or information systems unless the written approval of the Director of Information Technology has first been obtained. Before any third party or business partner is given access to this UACCM computers or information systems, a chain of trust agreement defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization.

1.1.6 Unauthorized Access: Users are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems.

System privileges allowing the modification of 'production data' must be restricted to 'production' applications.

1.1.8 Remote Access: Remote access must conform at least minimally to all statutory requirements including but not limited to HCFA, HRS-323C, FERPA, and HIPAA.

1.2 Workstation Access Control

1.2.1 All workstations used for UACCM business and educational activity, no matter where they are located, must use an access control system approved by UACCM. In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU and BIOS. Active workstations are not to be left unattended for prolonged periods of time, where appropriate. When a user leaves a workstation, that user is expected to properly log out of all applications and networks. Users will be held responsible for all actions taken under their sign-on. Where appropriate, inactive workstations will be reset after a period of inactivity (typically 30 minutes). Users will then be required to re-log on to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.

1.2.2 Disclosure Notice: A warning notice will be displayed initially before signing on to the system. The warning message will make clear that the system is a private network or application and unauthorized users should disconnect or log off immediately.

1.2.3 System Access Controls: Access controls will be applied to all computer-resident information based on the UACCM *Data Classification Policy* to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

1.3 Access Approval

System access will not be granted to any user without appropriate approval. Management is to immediately notify the UACCM Help Center and report all significant changes in end-user duties, employment status, or enrollment. User access is to be immediately revoked if the individual is no longer associated with UACCM. In addition, user privileges are to be appropriately changed if the user is transferred to a different job or department.

1.4 Limiting Access

1.4.1 UACCM approved access controls, such as user logon scripts, menus, session managers and other access controls will be used to limit user access to only those network applications and functions for which they have been authorized.

1.4.2 Need-to-Know: Users will be granted access to information on a "need-to-know" basis. That is, users will only receive access to the minimum applications and privileges required performing their jobs.

1.4.3 Compliance Statements: Users who access to this UACCM's information systems must sign a compliance statement prior to issuance of a user-ID. A signature on this compliance statement indicates the user understands and agrees to abide by these UACCM policies and procedures related to computers and information systems. Annual confirmations will be required of all system users.

1.5 Auditing

1.5.1 Logging and auditing trails are based on the Data Classification of the systems.

1.5.2 Confidential Systems: Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account
- Method of access
- All privileged commands must be traceable to specific user accounts

In addition logs of all inbound access into UACCM's internal network by systems outside of its defined network perimeter must be maintained. Audit trails for confidential systems should be backed up and stored in accordance with UACCM back-up and disaster recovery plans. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. All logs must be audited on a periodic basis and audit results should be included in periodic management reports.

Revision History

Date of Change	Responsible	Summary of Change
8/26/2019	Stephen Wallace	Initial creation of document