United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

DOI Museum Property Directives

Title: Museum Collection Management System (MCMS) Access Controls
Directive Number: 18.2
Originating Office: Office of Acquisition and Property Management
U.S. Department of the Interior (DOI)
Approved By: Megan Olsen
Official Title: Director, Office of Acquisition and Property Management
Effective Date: September 26, 2024
Expiration Date: This Directive will remain in effect until superseded.

MEGAN OLSEN

Digitally signed by MEGAN OLSEN
Date: 2024.09.26 13:01:03 -04'00'

2.1 **Purpose**. To establish access control policy and procedures for MCMS, pursuant to DOI Museum Property Directive 18.1, *Museum Collection Management System (MCMS)***,** and National Institute of Standards and Technology (NIST) requirements. These procedures will facilitate the implementation of the security control requirements for the Access Control (AC) family, as identified in NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*[1] and the Office of Management and Budget Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*.

2.2 **Scope**. This policy applies to all MCMS users, which includes DOI employees, contractors, interns, volunteers, and staff of non-DOI facilities that use MCMS to manage museum collections on behalf of DOI. This document defines the requirements for assigning, maintaining, and managing MCMS user accounts.

2.3 **Responsibilities**. The roles and responsibilities applicable to this Directive are documented in Directive 18.1.

2.4 **Account Management**.[2] MCMS user accounts are created, enabled, modified, maintained, disabled, and removed in accordance with these procedures. For specific procedures, see MCMS user documentation.

[1] Throughout the document, required controls are footnoted by the applicable code. For instance, AC-05 refers to the NIST Standard Access Control, control number 5.
[2] AC-02.f: Account Management. The organization creates, enables, modifies, disables, and removes information system accounts in accordance with system owner defined procedures or conditions.

A. Account Security Groups. Security in MCMS is applied at the unit level. Users for a unit will be assigned to a specific security group (i.e., certain permissions) for that unit. MCMS includes the following security groups:

(1) Cataloger. Limited data entry rights to a specific unit.

(2) Conservator. Limited data entry rights to a specific unit.

(3) Collections Manager. Data entry rights to a specific unit.

(4) Curator. Limited full rights to a specific unit.

(5) Custodial Property Officer. Full rights to a specific unit.

(6) Support. View access to specific units.

(7) Support Super User. Limited full rights to a specific unit.

(8) Internal Researcher. View access to specific areas of a specific unit.

(9) Restricted. No rights to a specific unit.

(10) System Administrator. DOI-wide system administration.

B. Exceptions. In limited circumstances, specific changes to the security controls may be authorized for individual user accounts. If a User requires a level of access higher than their current account allows, their account will be reviewed for increased access.

C. High-Level Workflow for **DOI User** Account Creation/Modification.[3]

(1) User access need is identified by the User and Supervisor.

(2) User completes all required training.

(3) User's Supervisor reviews and recommends the request.

(4) Accountable Property Officer reviews and authorizes the request.

(5) Supervisor submits user account request to the appropriate Account Manager.[4]

[3] AC-02.h.3: Account Management. The organization notifies Account Managers when information system usage or need-to-know changes for Users.

[4] AC-06: Least Privilege. When requesting/modifying a user account, Supervisors and Users should only request the least privilege that is necessary to accomplish the User's assigned tasks.

(6) Account Manager approves the request, approves the request with modifications, or rejects the request.

(7) Account Manager creates the account and notifies the User and Supervisor.

(8) Account Manager monitors the user account in accordance with Section 2.5 and retains the documentation and request for three years.[5]

D. High-Level Workflow for **Non-DOI User** Account Creation/Modification.

(1) User access need is identified by the User.

(2) User completes all required training.

(3) Sponsor is identified. A User only needs one Sponsor, even if they hold museum collections for multiple units within a single bureau or for multiple bureaus/offices within DOI.

(4) Sponsor submits the request to the MCMS Administrator.

(5) MCMS Administrator determines which bureau/office data the User will access and obtains concurrence from the applicable Bureau/Office Account Managers.

(6) MCMS Administrator approves the request, approves the request with modifications, or rejects the request.

(7) MCMS Administrator creates the account and notifies the User and Sponsor.

(8) MCMS Administrator monitors the user account in accordance with Section 2.5 and retains the documentation and request for three years.[6]

E. Account Manager Designations.

(1) Account Manager need is identified.

(2) Proposed Account Manager completes all required training.

(3) Bureau/Office Account Manager reviews and submits all Account Manager requests to the MCMS Administrator.

[5] AT-04: Training Records & General Records Schedule (GRS) 3.2: Information Systems Security Records. Documents the requirements for retention.

[6] AT-04: Training Records & GRS 3.2: Information Systems Security Records. Documents the requirements for retention.

(4) MCMS Administrator reviews the request and, if approved, completes the MCMS user setup as requested.

(5) MCMS Administrator notifies the Bureau/Office Account Manager and the new Account Manager that the account is established with instructions for logging in.

(6) MCMS Administrator retains the documentation and request for three years.[7]

F. User Account Requirements.

(1) Rules of Behavior. All MCMS users (DOI and non-DOI) must certify acceptance and compliance with the *MCMS Rules of Behavior*, which enhance and further define the specific rules each User must follow when using MCMS, in addition to DOI information management and security policies and procedures.

(2) Training.[8]

(a) All MCMS users (DOI and non-DOI) must complete DOI's Information Management and Technology (IMT) Awareness Training before requesting access to the system and annually thereafter.[9]

(b) MCMS training requirements are based on account security groups identified in Section 2.4A. Additional MCMS course requirements for specific roles are detailed in MCMS user documentation.

G. Disabling and Removing User Accounts.[10]

(1) Accounts will be disabled or removed by the Account Manager when any of the following conditions are met:

(a) User has not logged into MCMS in over 60 days.

(b) User training is past due.

[7] AT-04: Training records & GRS 3.2: Information Systems Security Records. Documents the requirements for retention.
[8] AT-03: Role-Based Training. The organization provides role-based training to defined Users.
[9] Available at: https://www.doi.gov/doitalent/training-download. DOI Users complete annually in DOI Talent to maintain Active Directory access.
[10] AC-02.h.1 & 2: Account Management. The organization notifies Account Managers: 1) When accounts are no longer required; 2) When Users are terminated or transferred. AC-02.f: Account Management. The organization disables and removes information system accounts in accordance with system owner defined procedures or conditions.

(c) User account has expired or is in violation of organizational policy.

(d) User account is requested to be disabled or removed.

(e) User is identified as a high-risk individual.[11]

(2) Accounts will be disabled by the appropriate Account Manager. Accounts will only be removed by the MCMS Administrator.

(3) Users are responsible for keeping their accounts active.

(4) Supervisors and Sponsors are responsible for monitoring any change in employment and/or duties that necessitate disabling or removing the user account and notifying the account manager within 60 days.

(5) Accountable Property Officers are accountable for ensuring all user access to their data is appropriate and will review the User Profile Report quarterly and the Audit Trail Report as necessary to identify issues.

(6) MCMS Administrator and Account Managers will review the Manage User Log quarterly.

2.5 **Monitoring**.[12]

A. User Profile Report. The User Profile Report lists the security and options profile for each User. The User Profile Report can be generated for a single user account or multiple accounts.

(1) Accountable Property Officers will review the User Profile Report on a quarterly basis, verify completion, and submit any necessary user account changes to the Account Manager.

(2) Account Managers and the MCMS Administrator will ensure all User Profile Reports are reviewed quarterly and take any necessary actions.

B. Manage User Log. The Manage User Log provides a listing of all system user access and includes the User ID and time stamps for each time Users log in and out of the system. The Manage User Log can be filtered for a specific date range and/or User. MCMS Administrator and Account Managers will review the Manage User Log on a quarterly basis and take any necessary follow up actions, including:

[11] AC-02(13): Disable accounts of high-risk individuals.
[12] AC-02.g: Account Management. The organization monitors the use of information system accounts.
AC-02.j: Account Management. The organization reviews accounts for compliance with account management requirements.

(1) Disable any accounts that have not been accessed in >60 days and notify the user, and

(2) Notify any users who have not accessed their account in >45 but <60 days that their account will be disabled soon.

C. Audit Trail Report. The Audit Trail Report lists additions, deletions, and modifications to data made by an MCMS User. Supervisors, Sponsors, Accountable Property Officers, Account Managers, and the MCMS Administrator will review the Audit Trail Report as needed.

APPENDIX A

MCMS RULES OF BEHAVIOR

Purpose: The Museum Collection Management System (MCMS) is an official United States Government system, owned by the U.S. Department of the Interior (DOI) that must be used only for authorized purposes. Rules of Behavior enhance and further define the specific rules each user must follow when using MCMS, in addition to complying with DOI information management and security policies and procedures.

Applicability: The MCMS Rules of Behavior are applicable to all users and at all levels of function and system privilege, including DOI employees, contractors, interns, volunteers, and staff at non-DOI facilities that manage museum collections on behalf of DOI.

Instructions: As a MCMS user, you must agree to these Rules of Behavior prior to being granted access to MCMS. You are accountable for your actions and responsible for the security of the information contained in MCMS. Upon being granted access to MCMS, you will be held responsible for damage caused to information either through negligence or a willful act. Failure to follow these rules will result in punitive measures, inclusive of that may include loss of access privileges, disciplinary action, and applicable legal proceedings.

As a MCMS user, I will:

1. Comply with Rules of Behavior for DOI computer network users, including successfully completing the initial and annual Information Management and Technology (IMT) Awareness Training (available to DOI users through DOI Talent and non-DOI users at https://www.doi.gov/doitalent/training-download).

2. Consent to monitoring and have no expectation of privacy when using Government computer equipment and/or the DOI computer network.

3. Operate the system in accordance with official training, MCMS user documentation and DOI and bureau/office policy and guidance.

4. Report any non-functional components or critical flaws to the MCMS Administrator and my Account Manager.

5. Not attempt to alter, bypass, and/or disable system configurations and security settings.

6. If granted any form of administrator or Account Manager access, operate only within approved frameworks, and will not alter system elements without approval from the MCMS Administrator.

7. Take all appropriate and reasonable precautions to protect privacy, Personally Identifiable Information (PII), Sensitive PII (SPII), and Controlled Unclassified Information (CUI) as defined in DOI policy.

8. Download and export information for official purposes only.

9. Handle and retain records in accordance with information classifications and records management requirements; and properly destroy records in accordance with records disposition schedules.

10. Immediately report suspected security incidents to my Supervisor or Sponsor, Accountable Property Officer, and Account Manager and provide full cooperation in accordance with DOI or bureau/office incident response procedures.

11. Seek technical assistance as needed.

12. Ensure I stay current on all training requirements and keep my account active by logging in every 60 days.

13. Notify my Supervisor or Sponsor to have my account disabled when I no longer need access.

Disclosure of PII, SPII, and CUI without supervisory authorization is prohibited by Part 470 of the Departmental Manual (DM), Chapter 1.7A. Further, 383 DM 9 prescribes standards for managing Privacy Act Records within DOI and reiterates statutory violations that any officer or employee who knowingly and willfully makes an unauthorized disclosure of records subject to the Privacy Act, or who willfully maintains a system of records without meeting the Act's notice requirements (5 U.S.C. 552a (e)(4)), is guilty of a misdemeanor and may be fined up to $5,000. Misuse of CUI related to the location and nature of resources threatens, damages, or destroys cultural or natural resources and is a violation of Federal property and resource protection laws.