



# United States Department of the Interior

OFFICE OF THE SECRETARY

Washington, DC 20240

## DOI Museum Property Directives

---

**Title:** Museum Collection Management System (MCMS)

**Directive Number:** 18.1

**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**Expiration Date:** This Directive will remain in effect until superseded.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  
13:00:21 -04'00'

- 1.1 **Purpose.** To provide policy on MCMS, the DOI collection management system used to document all bureau/office museum property (museum collections) and specific collection management activities. MCMS is intended to:
- A. Provide DOI with a cloud-based, enterprise solution for managing DOI museum collections that aligns with DOI's workflows.
  - B. Meet Federal cybersecurity requirements and information management standards.
  - C. Ensure uniform record keeping, as defined in DOI Museum Property Directive 3, *Required Standards for Documenting Museum Property*, of DOI museum collections data for accountability and resource management purposes, in support of collection management, research, resource stewardship, public outreach and education, and other uses of DOI museum collections.
  - D. Provide data to leadership to support oversight of bureau/office museum programs.
  - E. Track the status and condition of DOI museum objects for collection management and reporting purposes.
  - F. Facilitate the discoverability and sharing of museum collections data to support interaction, collaboration, consultation, and partnerships among DOI bureaus/offices, Indian tribes, partner institutions, affiliated and descendant communities, and the public.

- G. Provide appropriate access to museum collections data through account management controls established in DOI Museum Property Directive 18.2, *Museum Collection Management System (MCMS) Access Controls*.
  - H. Protect Controlled Unclassified Information, including Personally Identifiable Information and sensitive resource information pursuant to legal authorities and policy standards (See Privacy Impact Assessment, System of Records Notice).
- 1.2 **Scope.** This policy applies to all bureaus and offices responsible for managing museum collections.
- 1.3 **Definitions.** A list of definitions for the Departmental Manual, Part 411, *Identifying and Managing Museum Property* (411 DM) and the DOI Museum Property Directives is available in *Glossary*.
- 1.4 **Responsibilities.**<sup>1</sup>
- A. Deputy Assistant Secretary for Budget, Finance, Grants and Acquisition serves as the authorizing official for MCMS.
  - B. Director, Office of Acquisition and Property Management, as the **system owner** for MCMS:
    - (1) Provides oversight and management for the overall system acquisition, development, and integration, in addition to ongoing maintenance, system, and server updates.
    - (2) Issues and maintains MCMS user documentation.
    - (3) Designates the MCMS Program Manager.
    - (4) Delegates duties to the Associate Director, Asset Management, or the Manager, Interior Museum Program, as appropriate.
  - C. Heads of Bureaus and Offices and the Assistant Secretary - Indian Affairs.
    - (1) Ensure MCMS is used to document museum collections and that required standards are met.

---

<sup>1</sup> AC-05: Separation of Duties. The organization a) separates duties of individuals, as necessary, to prevent malevolent activity without collusion; b) documents separation of duties of individuals; and c) defines information system access authorizations to support separation of duties. These procedures will facilitate the implementation of the security control requirements for the Access Control (AC) family, as identified in National Institute of Standards and Technology (NIST) Special Publication 800-53, [Security and Privacy Controls for Information Systems and Organizations](#), and the Office of Management and Budget Memorandum M-22-09, [Moving the U.S. Government Toward Zero Trust Cybersecurity Principles](#).

- (2) Develop plans to ensure full implementation of MCMS in coordination with the system owner.

D. Senior Museum Property Officials.<sup>2</sup>

- (1) Evaluate best practices for using MCMS and ensure system use is consistent across DOI.
- (2) Designate Bureau/Office Account Managers.
- (3) Request the system owner authorize the MCMS Administrator to provide account management services, if applicable.<sup>3</sup>

E. Manager, Interior Museum Program, as the **MCMS Program Manager:**

- (1) Develops, oversees, and manages the DOI MCMS budget.
- (2) Designates and supervises the MCMS Administrator.

F. MCMS Administrator.

- (1) Monitors compliance with MCMS user documentation.
- (2) Coordinates with the MCMS Program Manager and MCMS Governance Panel to develop, update, and disseminate MCMS user documentation.
- (3) Coordinates customizations to the system with input from the MCMS Governance Panel.
- (4) Facilitates MCMS Governance Panel meetings.
- (5) Serves as Account Manager and back-up for Bureau/Office Account Managers.
- (6) Approves and implements, or rejects, all Account Manager requests for bureaus/offices.
- (7) Serves as Account Manager for all non-DOI users.
- (8) Performs system administration and configuration tasks in MCMS.

---

<sup>2</sup> The Senior Executive with oversight of bureau/office museum programs; also serves on the Executive Museum and Preservation Council.

<sup>3</sup> In cases where the system owner accepts account management responsibilities, the MCMS Program Manager and MCMS Administrator will assume these responsibilities. Generally, this support service will be for bureaus/offices with limited collections and staff or as interim back-up for bureaus/offices.

- G. Information Security Systems Officer (ISSO).
- (1) Conducts monthly and annual audits of user activity to identify risks, threats, and breaches.
  - (2) Monitors DOI sponsorship of FedRAMP authorization of software.
- H. MCMS Governance Panel.
- (1) Reviews and recommends proposed system changes and enhancements for development to the MCMS Program Manager.
  - (2) Recommends MCMS user documentation revisions to ensure data management and system operations meet mission objectives and data and security standards.
- I. Bureau/Office Account Managers.<sup>4</sup>
- (1) Manage all user accounts within the respective bureau/office.
  - (2) Designate Regional and/or Unit Account Managers and submit requests to the MCMS Administrator for approval.
  - (3) Define the appropriate portfolio of units/accounts for Regional and/or Unit Account Managers.
  - (4) Serve as back-up to Regional and Unit Account Managers.
  - (5) Approve and implement, or reject, user access requests.
  - (6) For all user accounts in their portfolios, conduct quarterly reviews of the Manage User Log and User Profile Report, and disable inactive accounts.
    - (a) Confirm review of user accounts by Regional and/or Unit Account Managers.
    - (b) Any accounts not reviewed by a Regional and/or Unit Account Manager remain the responsibility of the Bureau/Office Account Manager.
  - (7) For non-DOI user access requests, provide concurrence for or objections to account creation to the MCMS Administrator.

---

<sup>4</sup> AC-02.b: Account Management. The organization assigns Account Managers for information system accounts.

- (8) Report security issues and risks to the MCMS Administrator and ISSO.

J. Regional Account Managers.

- (1) Manage all user accounts within the respective region (or equivalent).
- (2) Serve as back-up to Unit Account Managers.
- (3) Approve and implement, or reject, user access requests.
- (4) For all user accounts in their portfolios, conduct quarterly reviews of the Manage User Log and User Profile Report, and disable inactive accounts.
  - (a) Confirm review of user accounts by Unit Account Managers.
  - (b) Any accounts not reviewed by a Unit Account Manager remain the responsibility of the Regional Account Manager.
- (5) Report security issues and risks to Bureau/Office Account Manager, MCMS Administrator, and ISSO.

K. Unit Account Managers.

- (1) Manage all user accounts within the respective unit.
- (2) Approve and implement, or reject, user access requests.
- (3) For all user accounts in their portfolios, conduct quarterly reviews of the Manage User Log and User Profile Report, and disable inactive accounts.
- (4) Report security issues and risks to the Regional Account Manager, Bureau/Office Account Manager, MCMS Administrator, and ISSO.

L. Supervisors.

- (1) Assess the type and level of access required for employees, interns, volunteers, and supporting contractors<sup>5</sup> in the area(s) of responsibility and ensure there are no separation of duties<sup>6</sup> conflicts.
- (2) Review and recommend access requests to the Account Manager.

---

<sup>5</sup> For contractors, this is the Contracting Officer's Representative (COR). For agreement participants, this is the Agreements Technical Representative (ATR).

<sup>6</sup> AC-05: Separation of Duties. The organization a) separates duties of individuals, as necessary, to prevent malevolent activity without collusion; b) documents separation of duties of individuals; and c) defines information system access authorizations to support separation of duties.

- (3) Monitor MCMS access of DOI users via normal supervision activities, Audit Trail Report, User Profile Report, and Manage User Log.
- (4) Keep the Accountable Property Officer informed of MCMS access and use for the unit.

M. Sponsors.

- (1) Are permanent DOI employees.
- (2) Sponsor non-DOI users for MCMS access and assess the type and level of access required.
- (3) Submit MCMS access requests to the MCMS Administrator on behalf of non-DOI users.

N. Accountable Property Officers.

- (1) Review and authorize user access to museum collections data within the scope of responsibility.
- (2) Review the User Profile Report on a quarterly basis to ensure all active accounts are in use and verify review to the Account Manager.
- (3) Delegate duties and responsibilities to the appropriate Custodial Property Officers, if applicable.

O. Users, including DOI employees, contractors, interns, volunteers, and staff of non-DOI facilities that manage museum collections data on behalf of DOI.

- (1) Maintain current training and comply with MCMS user documentation.
- (2) Abide by all museum collections data management requirements for the security and integrity of the museum collections data.
- (3) Submit MCMS access requests to Supervisors/Sponsors.
- (4) Access and operate the system in accordance with *MCMS Rules of Behavior*.
- (5) Report security risks, threats, and breaches to Supervisors, Sponsors, applicable Account Managers, and the MCMS Administrator.

1.5 **Standards.** 411 DM provides general requirements for the use of MCMS for documenting DOI museum collections. The required standards and mandatory data to document museum collections are found in the DOI Museum Property Directives.

MCMS includes data fields, functions, and reports to meet the mandatory documentation standards.

**1.6 Use of MCMS.**

- A. DOI staff must use MCMS to document all bureau/office museum collections data and specific collection management activities.
- B. Bureaus/offices must use the data in MCMS, as practicable, to fulfill museum collections reporting requirements as stated in 411 DM, audit requests, and any additional requests/requirements.
- C. Staff at any non-DOI facility housing DOI museum collections may use MCMS to manage DOI museum collections data under the DOI MCMS contract and software license as defined in specific agreements.

**1.7 Bureau/Office Policy.** All bureaus/offices with museum collections must determine if additional MCMS user documentation specific to the use of MCMS is needed to address requirements in further detail. This may include, but is not limited to, bureau/office security requirements, data updates, use of reports, and data conversion and migration.

**1.8 Account Management.** Account management will be performed in accordance with this policy and Directive 18.2.

**1.9 Instruction and Technical Support.**

- A. User Documentation. MCMS user documentation for use of all MCMS features and functions is available to all bureaus/offices and non-DOI facilities managing DOI museum property.
- B. Technical Support. MCMS technical support, including all updates to the MCMS software, is provided under the DOI MCMS contract for all DOI users and all users in non-DOI facilities managing DOI collections. The MCMS vendor will provide support for technical and procedural questions on MCMS according to the DOI MCMS contract.
- C. Training. DOI-wide training in the use of MCMS is provided by the Interior Museum Program. Bureaus/offices may also develop MCMS training specific to their needs. The MCMS Administrator is available to assist bureaus/offices with specialized training according to the DOI MCMS contract.