

**FISH AND WILDLIFE SERVICE
FINANCE**

TABLE OF CONTENTS

Topics	Sections
<u>OVERVIEW</u>	4.1 What is the purpose of this chapter? 4.2 What is the scope of this chapter? 4.3 What is the overall policy? 4.4 What are the authorities for this chapter? 4.5 What terms do you need to know to understand this chapter? 4.6 How do role assignments in the Financial and Business Management System (FBMS) work?
<u>RESPONSIBILITIES</u>	4.7 Who is responsible for the elements of the Service's FBMS access policy?
<u>REQUIREMENTS</u>	4.8 What Departmental information technology security requirements drive the policy in this chapter? 4.9 What does the Department recommend as the best practice for system inactivity? 4.10 How often is FBMS access and use monitored? 4.11 What are some examples for which an employee's access may be removed? 4.12 Can the Service grant an exception to this policy?

OVERVIEW

4.1 What is the purpose of this chapter? This chapter describes the U.S. Fish and Wildlife Service's (Service) requirements for employees to continue to retain access to the Financial and Business Management System (FBMS) and for removal of end user roles.

4.2 What is the scope of this chapter?

A. This chapter applies to all Service accounts in FBMS. FBMS is the financial system of record for the Department of the Interior (Department).

B. For cross-servicing users (i.e., users who perform work in FBMS for more than one bureau), this chapter applies only to their Service FBMS account.

4.3 What is the overall policy?

A. How FBMS is organized: FBMS is made up of subsystems (e.g., Core Financials, PRISM). In each subsystem there are many roles (e.g., ACQ_REQ, AP_DCM, CC_BFO) that employees use to access the subsystem depending on what they are doing. An employee may have one role to access a subsystem or several.

B. Access requirement: Our policy requires FBMS users to log on to and use each subsystem of FBMS for which they need access at least once every 365 days. Users do not have to use every role they are assigned within that 365 days, but they must use at least one of their roles to enter the subsystem to retain their access.

(1) For any FBMS user who has not accessed any subsystem in FBMS for the previous 365

**FISH AND WILDLIFE SERVICE
FINANCE**

Finance

Part 260 Financial Management

Chapter 4 Retaining FBMS Access

260 FW 4

days, all of the user's roles will be removed and their user identification (ID) will be deactivated. However, if a user requests and receives an automated report(s) from FBMS that he/she had to act on, he/she will not lose access.

(2) If an FBMS user accesses and uses one subsystem, but not another, for the previous 365 days, he/she will retain access to the subsystem used and lose access to the unused subsystem(s). All of his/her roles will be removed for the unused subsystem(s).

(3) If, for the past 45 days, an FBMS user accesses and uses one subsystem, but does not access another, he/she will retain access to the subsystem used and automatically lose access to the unused subsystem(s). All of his/her roles will remain intact, but he/she must contact the Regional Account Controller to be unlocked.

4.4 What are the authorities for this chapter?

- A. [Departmental Security Control Standard, Access Control](#), Version 4.1, September 2016.
- B. Federal Information Security Modernization Act of 2014 (FISMA) ([44 U.S.C 3553](#)).
- C. [National Institute of Standards and Technology \(NIST\) Special Publication 800-53 Rev. 4; Security and Privacy Controls for Federal Information Systems and Organizations; April 2013 and updated January 22, 2015.](#)
- D. [Office of Management and Budget \(OMB\) Circular A-123](#), Management's Responsibility for Internal Control.
- E. [OMB Circular A-130, Revised](#), Transmittal Memorandum No. 4, Management of Federal Information Resources.

4.5 What terms do you need to know to understand this chapter?

A. Business Integration Office (BIO). The BIO, an office within the Department, supports the integration of new or modified business systems that focus on those business functions within the Department that report to the Deputy Assistant Secretary – Budget, Finance, Performance, and Acquisition (DAS-BFPA). This includes sustainment of FBMS. The BIO, as a shared service provider, uses FBMS and other assigned business systems to support all bureaus and offices in business functions such as core accounting, budget execution, acquisition, real property, etc.

B. Financial and Business Management System (FBMS). FBMS is the official financial management system of the Department. It is a Systems, Applications, and Products (SAP) in data processing-based, off-the-shelf enterprise resource planning system that integrates the Department's financial management functions into a single system. FBMS supports business management processes related to financial management, budget execution, acquisition, grants and cooperative agreements, real and personal property management, fleet management, aviation, travel, enterprise information management, and reporting.

C. FBMS Account Controller. FBMS Account Controllers are the security approvers for an assigned area. They are responsible for reviewing and approving role assignments and

**FISH AND WILDLIFE SERVICE
FINANCE**

Finance

Part 260 Financial Management

Chapter 4 Retaining FBMS Access

260 FW 4

revocations of users within their areas of accountability. To assign or remove roles from a user in FBMS, both the FBMS Account Controller and Security Point of Contact (SPOC) must approve it.

D. FBMS inactivity. FBMS inactivity occurs when a user has not performed an action in any of the FBMS subsystems (e.g., running a report in the Enterprise Management Information System (EMIS) or entering financial data into Core Financials) within a 365-day time frame. Logging into the FBMS portal, but not using any of the subsystems, does not prove activity. You have to use the subsystem. Users who schedule reports regularly in FBMS and have them automatically emailed remain active if they act on the reports more than once every 365 days.

E. FBMS portal. The FBMS portal is also referred to as the FBMS frontend. It provides access or links to subsystems within FBMS depending on a user's approved roles. The portal does not contain transactional or financial data, but may include user guides, training materials, and general information about the system.

F. FBMS security personnel. FBMS security personnel, include, but are not limited to:

- (1) FBMS Account Controllers,
- (2) FBMS Internal Control Coordinators,
- (3) FBMS Mitigating Control Monitors,
- (4) FBMS Regional Managers,
- (5) FBMS SPOCs, and
- (6) FBMS Training Coordinators.

G. FBMS Security Point of Contact (SPOC). SPOCs support the management and administration of users in FBMS by monitoring, approving, and removing users and user role assignments. FBMS SPOCs interact frequently with the BIO security team and the FBMS security teams from other bureaus and offices.

4.6 How do role assignments in FBMS work?

A. Every user is issued a unique user ID, which is associated with one or many roles. When a user initially requests access to FBMS, the ID that is created for the user is associated with the user's Active Directory ID. This is done so that when the user logs in to FBMS, all of the mapped user information, such as the roles assigned to the user in the subsystems, are automatically known, and FBMS enables a single sign-on to these applications.

B. Each role is made up of a collection of authorizations that define which subsystems a user may access and which actions a user may perform. These roles also define the type of data the user may access, such as limiting access to Service data only.

**FISH AND WILDLIFE SERVICE
FINANCE**

(1) FBMS security personnel request the initial roles assigned to a user by using the User Account Management (UAM process), which is automated using the Governance, Risk, and Compliance (GRC) module in FBMS. They also use GRC to make changes to those roles.

(2) The roles may not necessarily map to a specific job title, but instead relate to the user’s anticipated duties in FBMS, and they are usually based on steps within a business process.

RESPONSIBILITIES

4.7 Who is responsible for the elements of the Service’s FBMS access policy? See Table 4-1.

Table 4-1: Responsibilities Related to the FBMS Access Policy

These employees...	Are responsible for...
A. The Director	Ensuring that our financial management systems comply with Federal policies and standards.
B. Assistant Director – Business Management and Operations	Making sure there is adequate policy in place so that access to FBMS is controlled as required by Departmental and Federal policy.
C. Assistant Director – Information Resources and Technology Management (i.e., the Associate Chief Information Officer)	Advising employees on the security and implementation of financial management systems.
D. Directorate members (e.g., Assistant Directors, Regional Directors)	Ensuring that those employees for whom they are responsible comply with the requirements in this chapter.
E. Chief, Division of Financial Management (DFM)	Disseminating the latest Federal and Departmental policy and providing guidance to Service personnel on financial management system requirements.
F. FBMS Bureau Lead (Branch of Business Integration (BBI), DFM)	(1) Keeping this policy up-to-date, and (2) Overseeing FBMS use to ensure compliance with this policy.
G. FBMS Account Controllers (DFM, Regions)	(1) Reviewing user activity lists for their areas of responsibility, (2) Reminding users about access and use requirements, as needed, and (3) Removing roles and deactivating accounts for users who have not used FBMS for the previous 365 days.
H. FBMS SPOCs (BBI, DFM)	(1) Generating reports regarding user activity and providing them to the Account Controllers on a monthly basis for any users who have not used their FBMS subsystem(s) within the past 365 days,

**FISH AND WILDLIFE SERVICE
FINANCE**

Finance

Part 260 Financial Management

Chapter 4 Retaining FBMS Access

260 FW 4

These employees...	Are responsible for...
	<p>(2) Monitoring the removal and deactivation task until completion, and</p> <p>(3) Supporting the Account Controllers, when necessary, by removing roles and deactivating accounts as we require in this policy.</p>

REQUIREMENTS

4.8 What Departmental information technology security requirements drive the policy in this chapter?

A. The Department requires that we monitor and control all information technology/system user accounts. The Departmental [Security Control Standard, Access Control](#) requires us to:

- (1)** Identify and select the types of information system accounts we need to support organizational missions/business functions (i.e., individual, group, system, application, guest/anonymous, and temporary);
- (2)** Assign account managers for information system accounts;
- (3)** Establish conditions for group and role membership;
- (4)** Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- (5)** Require approvals from account managers for requests to create information system accounts;
- (6)** Create, enable, modify, disable, and remove information system accounts in accordance with the procedures or conditions the system owner defines;
- (7)** Monitor the use of information system accounts;
- (8)** Notify account managers when:
 - (a)** Accounts are no longer required,
 - (b)** Users separate or are terminated or transferred, and
 - (c)** Individual information system use or need-to-know changes;
- (9)** Authorize access to information systems based on:
 - (a)** A valid access authorization,

**FISH AND WILDLIFE SERVICE
FINANCE**

(b) Intended system use, and

(c) Other attributes that the organization or associated missions/business functions require;

(10) Review accounts for compliance with account management requirements at least annually; and

(11) Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

B. In addition to monitoring and controlling accounts, the Department requires that we ensure that users are only granted the amount of access they need to perform their jobs. A user should only be assigned roles that they need to complete their work assignments.

4.9 What does the Department recommend as the best practice for system inactivity? The guidance from the Department’s Office of the Chief Information Officer (OCIO) is that for a financial system such as FBMS, it is a best practice for users to have their roles removed and their ID deactivated in the system after the user has not used the system for between 180 and 365 days.

4.10 How often is FBMS access and use monitored? Following BIO policy and guidance, the FBMS security team (i.e., SPOCs) performs a user review quarterly. In addition to the BIO-mandated review, the FBMS security team performs a partial user review monthly to help with continuous monitoring.

4.11 What are some examples for which an employee’s access may be removed? See Table 4-2.

Table 4-2: “If-Then” Scenarios for Deactivation

In the following examples of user activity...	The following actions will be taken...
An employee last used his acquisition role in PRISM and Core Financials 365 days ago and last used EMIS 365 days ago.	All of the employee’s roles in FBMS will be removed and his ID will be deactivated. He will lose all access to FBMS.
An employee last used her acquisition roles in PRISM and Core Financials 2 days ago, but has not used EMIS for 365 days.	All of the employee’s roles in EMIS will be removed. She will retain her roles in PRISM and Core Financials and will not lose FBMS access.
An employee last used her acquisition and property roles in PRISM and Core Financials 2 days ago. She had an EMIS report that she reviews monthly and acts on emailed to her 15 days ago, but hasn’t entered EMIS for 365 days.	The employee will maintain all roles in PRISM/Core Financials/EMIS because she is using her access on a regular basis and needs the roles to perform her job.

**FISH AND WILDLIFE SERVICE
FINANCE**

Finance

Part 260 Financial Management

Chapter 4 Retaining FBMS Access

260 FW 4

4.12 Can the Service grant an exception to this policy? Yes, the FBMS Bureau Lead (i.e., BBI, DFM) may grant exceptions to this policy on a case-by-case basis. To request an exception, please contact your assigned Account Controller.

/sgd/ Stephen Guertin
DEPUTY DIRECTOR

Date: February 12, 2018