# Standard PR.AC: Separation of Duties

**February 10, 2021**

**U.S. Department of Education (ED)**

**Office of the Chief Information Officer (OCIO)**

**Information Assurance Services (IAS)**

**APPROVAL**

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.10 19:05:44 -05'00'

_____ _____

**Steven Hernandez** **Date**

**Director, IAS/Chief Information Security Officer (CISO)**

## Revision History

The table below identifies all changes that have been incorporated into this document.

| Version | Draft Date | Summary of Changes |
|---|---|---|
| 1.0 | 5/07/2019 | Initial draft |
| 1.1 | 06/03/2019 | Updated |
| 1.2 | 06/25/2019 | Updated to include separation of developer-role access to operational environments for financial systems and other High-Value Assets |
| 1.3 | 06/29/2019 | Referenced Financial System |
| 1.4 | 12/15/2019 | Underwent annual policy review for accuracy and timeliness and to incorporate updates to NIST SP 800-53 Rev. 4. No updates were required as of December 2019. |
| 1.5 | 1/25/2021 | Underwent annual policy review for accuracy and timeliness, updated exceptions section, and standardized risk acceptance/policy exception verbiage. |

# Table of Contents

# 1. INTRODUCTION

## 1.1. Purpose

This document establishes the Department's standards for the separation of duties within an information technology environment. In doing so, it supersedes any prior documentation establishing such standards.

## 1.2. Scope

The standard established in this document applies to all employees, contractors, and users authorized to access ED information systems, systems operated or maintained on behalf of ED, or ED information.

# 2. STANDARDS

- Information Security Management roles must be assigned to different individuals.
- Information System Owners (ISOs) must identify relevant IT roles within their Information System Security Plan.
- ISOs must identify within their Information System Security Plan how duties are to be separated so that critical IT functions are segregated to prevent any one person from having the authority or ability to harm or circumvent normal checks and balances of a development or an operational system or the services it provides, whether by accident, omission, or intentional act.
- ISOs must consider the potential for fraudulent activity in assigning and reviewing system access privileges.
- In determining the assignment of roles, ISOs and designees must:
    - Have at least two people involved within each process or sub-process
    - Have two people involved in certain controls, where necessary (i.e., at times a single control may be split into activities that are assigned to different individuals)
- Financial Systems categorized as high value assets (HVA), must ensure system development roles are distinctly segregated from production environments **NOTE:** *See Appendix B for the definition of a financial system.*
- The following, although not an exhaustive list, outlines additional responsibilities that should be considered incompatible and must be separated:

- Initiation of a transaction vs. approval of the same transaction
- Updating of vendor/employee records vs. approval of financial transactions related to that vendor/employee
- Processing of transactions vs. authorization of access to systems/applications.

### 2.1. Enforcement

Personnel who are responsible for managing system security (e.g., Information System Security Officers, Information System Owners, etc.) are accountable for the implementation of all separation-of-duty policies and should be documented in the implementation statement and supporting evidence of NIST SP 800-53 Rev 4 AC-05 Separation of Duties in the Information System Security Plan (SSP).

### 2.2. Exceptions

In instances in which it is impractical to have meaningful separation of duties due to limited staff, it may be necessary for a system owner to establish mitigating controls, which must be rigorously documented and followed. In such cases, direct managerial involvement provides a strong deterrent to potential conflicting activities/interests. Examples of such involvement include:

- Rotation of duties among personnel
- Increased hands-on supervision
- Enforced vacations
- Having a manager perform one aspect of the transaction (e.g., approving invoices, etc.)
- Active review by management of financial data and reports (e.g., reconciliations, voucher status report, appropriation status reports)
- A detailed management review of activities involving finances, inventory, and other assets must be required as a compensating control activity.
- Increased frequency of audit log review, especially for those logs generated from privileged user activities

## 3. RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

# APPENDIX A: References

- National Institute of Standards and Technology, *800-53 (as amended) Security Controls and Assessment Procedures for Federal Information Systems and Organizations; AC-5 Separation of Duties*

- National Institute of Standards and Technology, *800-53 (as amended) Security Controls and Assessment Procedures for Federal Information Systems and Organizations; AC-6 Least Privilege*

- Departmental Directive, OCFO 1-103; Financial Management

# APPENDIX B: Definition of a Financial System

**Per OCFO 1-103; Financial Management, the following is the definition of financial systems.**

*"**Financial Systems*** - Information systems comprised of one or more applications that are used for any of the following:

1. Collecting, processing, maintaining, transmitting, and reporting data about financial events;

2. Supporting financial planning or budgeting activities;

3. Accumulating and reporting cost information; or

*4.* Supporting the preparation of financial statements.*"*