Standard PR.AC: User Account Recertification

February 11, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to

OCIO_IAS@ed.gov

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.11 12:41:43 -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	7/10/2019	Initial draft
1.1	10/03/2019	Revised to clarify review frequencies for different system types.
1.2	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.
1.3	1/25/2021	Underwent annual policy review for accuracy and timeliness. Standardized risk acceptance/policy exception. Included OCIO account review attestation template reference.

Table of Contents

1. INTRODUCTION

1.1. Purpose

This document establishes the U.S. Department of Education (ED) standard for the review and recertification of privileged and non-privileged user accounts.

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. STANDARD

2.1. Overview

All ED information system user accounts (privileged and non-privileged) and service accounts must undergo regularly scheduled review to recertify and maintain their validity. To ensure this:

- Information System Owners (ISO) must conduct regular recertification reviews of user accounts based on system type and sensitivity-level, service accounts based on mission/business need, per the required frequencies of review described below.
- Information System Security Officers (ISSO) must confirm and certify that user account recertification reviews have occurred at the required frequencies for system type and sensitivity-level.
- ISSOs must review both ISO and Authorizing Officials' system account access to ensure separation of duties.

2.2. Process

The following describes the roles, responsibilities, and required process for the recertification of ED system user and service accounts. **NOTE:** After a System Administrator generates the Account Recertification Report, both the ISSO and ISO must review and sign the report to verify that all steps below were taken.

- In reviewing a system for recertification of user account access, **System Administrators** must:
    1. Produce a system-generated list of all user accounts and their levels of access and privileges.
    2. Send the list to the corresponding ISSO and ISO for their review.
    3. Take appropriate action to modify, lock, or terminate user access as indicated by the ISSO and ISO.

4. Prepare a report of user-account recertification results (User Account Recertification Report), corrective actions, and supporting documentation for review and approval by the ISSO and ISO. There is no specific required report format which must be used. A template which may be used is available in connectED; this template is titled **"Memorandum for the Record, Privileged and Non-Privileged User Account Recertification Report"**. Regardless of the report format used, the final report must include all required signatures.
5. Obtain ISSO and ISO signatures on the User Account Recertification Report, verifying that all steps described above were taken.

- In reviewing a system for recertification of user account access, **ISSOs and ISOs** must coordinate to:
    1. Upload the signed User Account Recertification Report to CSAM for each applicable system, per the AC-2 security control.
    2. Retain all user account recertification documentation for a full ATO lifecycle.
    3. Review and validate ***non-privileged*** user accounts and access annually.
    4. Review and validate ***privileged*** user accounts (including service accounts, machine accounts, power users, etc.):
        - **Monthly** for High Value Assets & High Impact systems
        - **Quarterly** for Moderate and Low Impact systems

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: RESOURCES AND REFERENCES

- NIST Special Publication (SP) 800-53, (as amended): *Security and Privacy Controls for Federal Information Systems and Organizations*