Standard PR.AC: User-Notification Warning Banner

May 18, 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 Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.05.18 16:18:50 -04'00'

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.

1.0	12/31/2018	Initial draft
1.1	12/9/2019	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.
1.2	1/13/2021	Underwent annual policy review for accuracy and timeliness. Updated scope, updated reference to Education Science Reform Act, and risk acceptance/policy exceptions verbiage.
1.3	5/18/2021	Updated Section 2 to include responsibility for Information System Owners (ISO) and Information System Security Officers (ISSO) for ensuring AC-08.

Table of Contents

1. INTRODUCTION 2

1.1 Purpose 2

1.2 Scope 2

2. STANDARD 2

3. RISK ACCEPTANCE/POLICY EXCEPTIONS 3

1. INTRODUCTION

1.1 Purpose

Department of Education information systems, websites, and applications with user text or graphic interfaces are required to display a Department-approved user-notification/warning banner before permitting user access. This document establishes a standard for the use of such a banner, and in doing so, it supersedes any prior documentation establishing such a standard.

1.2 Scope

The standards established in this document apply to all Department internet-accessible production web applications and websites except for Institute of Education Sciences' websites that adhere to the Education Science Reform Act[1].

2. STANDARD

Following is the standard warning banner/system-use notification that should be presented to users of internet-accessible production web applications and ED websites.

Warning

You are accessing a U.S. Federal Government computer system intended to be solely accessed by individual users expressly authorized to access the system by the U.S. Department of Education. Usage may be monitored, recorded, and/or subject to audit. For security purposes and in order to ensure that the system remains available to all expressly authorized users, the

U.S. Department of Education monitors the system to identify unauthorized users. Anyone using this system expressly consents to such monitoring and recording. Unauthorized use of this information system is prohibited and subject to criminal and civil penalties. Except as expressly authorized by the U.S. Department of Education, unauthorized attempts to access, obtain, upload, modify, change, and/or delete information on this system are strictly prohibited and are subject to criminal prosecution under 18 U.S.C § 1030, and other applicable statutes, which may result in fines and imprisonment. For purposes of this system, unauthorized access includes, but is not limited to:

Any access by an employee or agent of a commercial entity, or other third party, who is not the individual user, for purposes of commercial advantage or private financial gain (regardless of whether the commercial entity or third party is providing a service to an authorized user of the system); and

Any access in furtherance of any criminal or tortious act in violation of the

[1] Education Sciences Reform Public Law 107-279

Constitution or laws of the United States or any State.

If system monitoring reveals information indicating possible criminal activity, such evidence may be provided to law enforcement personnel.

NOTE: The Information System Owners (ISO) and Information System Security Officers (ISSO) are required to ensure that the Department standard warning banner/system-use notification is implemented through the System's Security Plan (SSP). The AC-08 (System Use Notification or Warning Banner) security control needs to be documented and implemented before an Authority to Operate (ATO) is issued or if during change management a new site or existing site is changed that would necessitate the re-validation that the AC-08 security control is still implemented and presented to users of internet-accessible production web applications and ED websites.

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).