Standard PR.AC: Emergency PIV-Alternative Standard

February 10, 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: 2021.02.10 19:07:00 -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	5/5/2020	Initial draft
1.1	2/10/2021	Reviewed for accuracy and timeliness. Updated approved use cases, PIV-A use case procedures and standardized Risk acceptance and Policy exception section.

Table of Contents

1 INTRODUCTION 1

1.1 Purpose 1

1.2 Scope 1

1.3 Background 1

2 STANDARDS 1

2.1 Approved Use Cases 1

2.2 Example PIV-A Use-Case Procedures 2

2.3 Revisions to PIV-A Standard 2

3. RISK ACCEPTANCE/POLICY EXCEPTIONS 2

APPENDIX A: RESOURCES AND REFERENCES 3

1 INTRODUCTION

1.1 Purpose

In order to address the closure and limited operating capacity of Federal Government badging offices due to the Coronavirus (COVID-19), this standard provides authorization to access Department of Education (Department or ED) systems for those who are unable and/or do not hold a valid Personal Identification Verification (PIV) but have been cleared by the Department's Office of Personnel Security. This guidance supersedes any prior documentation establishing such standards.

1.2 Scope

The standards established in this document apply to all employees, contractors, and users authorized to access ED's network and information systems.

1.3 Background

- The PIV card is the Department's standard for access to the Department's network and information systems.
- ED personnel who lack a valid PIV card are authorized to gain access to the Department's network and information systems through the alternative multifactor authentication standard solution.
- To gain access to the Department network and information systems without a PIV card, the Department has created a PIV-alternative solution (PIV-A) to allow personnel without PIV cards temporary access to ED's network and information systems using multifactor authentication. **This is a temporary exemption for use only in the specific cases listed in this document.**

2 STANDARDS

2.1 Approved Use Cases

As of this Standard's approval date, PIV-A is approved only for the duration of the current pandemic and only for use in the following cases:

- Expired or expiring PIV card(s)
- Expired PIV certificate(s)
- Lost PIV card(s)
- Damaged PIV card(s)
- Damaged PIV reader(s)

- Stolen PIV Card(s) (NOTE: Stolen PIV cards must be immediately reported to the relevant ISSO and the ED Security Operations Center [EDSOC])
- New personnel (Contractors and Federal employees) awaiting PIV card issuance
- Personnel requiring assistive technology (e.g., personnel qualifying under Section 508 of the Rehabilitation Act of 1973)
- Personnel required to use multiple devices simultaneously

2.2 Example PIV-A Use-Case Procedures

The following use-case procedures are cited as examples, however for the additional use-cases shown above.

- **Use Case 1**: ***PIV-A Request for a New User***
  1. IT POC receives new user account request.
  2. For Federal employees (and other users with non-GFE who require ED access), IT POC Determines PIV -A eligibility based on approved uses cases
  3. IT POC submits a service catalog request in ServiceNow.
  4. GFE is configured for PIV-A access and shipped to user.
  5. Enterprise Technology Services (ETS) tracks the request and provides continuous PIV-A tracking reports to the EDSOC.

- **Use Case 2: *PIV-A Request for Expiring or Expired PIV Card/Credentials***
  1. ED Personnel Security Office provides the OCIO IT POC with a list of individuals with expiring or expired PIV cards/credentials.
  2. ETS coordinates with the impacted end-user to implement PIV-A conversion.
  3. ETS tracks the request and provides continuous PIV-A tracking reports to the EDSOC.

2.3 Revisions to PIV-A Standard

This Standard may be revised, superseded, or fully rescinded based on guidance issued by the ED CISO. Specific questions related to the implementation of this Standard must be directed to the IAS_Governance@ed.gov mailbox.

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

- Department of Homeland Security: CISA, *Trusted Internet Connections 3.0 Interim Telework Guidance*, April 8, 2020