Standard PR.AC: Password Parameters

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

Approval

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.11 12:42:25 -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	5/31/2019	Initial draft
1.1	12/10/2020	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. Clarified the definition of machine accounts to include Active Directory accounts for laptop and desktop workstations.
1.2	2/12/2020	CISO Review and update
1.3	1/13/2021	Annual review for accuracy and timeliness. Updated policy exception verbiage.

Table of Contents

1. INTRODUCTION

This document establishes Department of Education standards for password parameters. In doing so, it supersedes any prior documentation establishing such standards.

NOTE: The mandatory standard for accessing ED information systems is via two-factor identification, using both a Personal Identity Verification (PIV) card **and** a Personal Identification Number (PIN).

System access using only a password without a PIV card is **only** permitted if PIV usage is not a technically viable option, such as on legacy systems lacks PIV capability. A PIV exemption risk acceptance form must be submitted to Information Assurance Services (IAS) for approval.

2. STANDARDS

Table 1 (below) details the ED password parameters for the following account types:

- **Individual User Accounts** - 'users' are defined in *OCIO: 3-112, Applicability*
- **Power User Accounts** - users who have access to other users' PII (e.g., Help Desk support)
- **Privileged User Accounts** - group accounts and role-based accounts (e.g., Administrator accounts) as defined by ED policy
- **Service Accounts** - accounts that an application or service uses to interact with other systems or services (e.g., the operating system)
- **Machine Accounts** - accounts that represent a server or client device in an Active Directory domain and only have machine-to-machine communication without user intervention. Machine accounts also include Active Directory domain accounts used to join a laptop, desktops and other workstations to the domain.

Table 1. ED Password Parameters

	Individual User Accounts	Power User Accounts	Privileged User Accounts	Service Accounts	Machine Accounts
Account Name	**N/A**	**N/A**	**N/A**	**N/A**	**Account names must not identify the role or function of the account.**
Password Complexity	**Passwords must be composed of a Passphrase. (Note: Spaces are counted as a character in the composition of a Passphrase.) Passphrases must be randomly chosen and cannot consist of commonly used phrases.** **If the system does not have the capability to implement a passphrase, the following password complexity must be implemented:** **Passwords must contain each of the following four types of characters:** **• English uppercase letters (A-Z)** **• English lowercase letters (a-z)** **• Arabic numerals (0-9)** **• Non-alphanumeric special characters ($,!, &, etc.)**	***Same as field at left***	***Same as field at left***	***Same as field at left***	***Same as field at left***

Minimum/Maximum Password Length	**Passphrases must be at least sixteen (16) characters in length or the longest password length the technology or product can support.** **If the system does not have the capability to implement a passphrase, the below password length will be implemented:** **Passwords must be at least twelve (12) characters in length. In instances where commercial technologies and products are unable to support 12 characters, the longest password that the specific commercial technology or product can support must be implemented.**	***Same as field at left**	***Same as field at left**	***Same as field at left**	**N/A**
Password Expiration **(How long a password can be used before the system requires it to be changed)**	**Passwords must be changed after 90 days of use. To support this, systems must be configured to accommodate a 5-day grace period during which the user may change their password. Specifically, parameters must place a "soft lock" on the account if the user does not log in on the 85th day of the password's life**	***Same as field at left**	***Same as field at left**	***Same as field at left**	**N/A**

	span, so that the user will have five days remaining to change the password.				
Account Lock-Out	**After three (3) consecutive unsuccessful login attempts, the account must be locked for the period of time specified by the Account Lock-Out Duration parameter.**	***Same as field at left***	***Same as field at left***	**System Accounts must be locked immediately upon any unsuccessful attempt to login.**	**N/A**
Account Lock-Out Duration	**An account will be locked out for 30 minutes, unless the User contacts the Help Desk to manually unlock the account during the 30 minutes.** **For systems unable to set the 30-minute lockout duration, accounts must remain locked until being reset by an administrator.**	***Same as field at left***	***Same as field at left***	**Until reset by an administrator.**	**N/A**
Disabling the account due to excessive account Lock-Out	**After three (3) consecutive account lock-outs due to unsuccessful login attempts (see Account Lock-Out parameter), the account must be disabled until an admin can re-enable it.**				

Minimum Password Age **(The minimum number of days a password must be in use before the user may change it.)**	**Passwords cannot be changed until they have been in use at least 5 days.** **For systems that cannot enforce the minimum password age, administrators must disallow reuse of all passwords used within the past year.**	***Same as field at left***	***Same as field at left***	**N/A**	**N/A**
Limitation of Password Reuse **(The minimum number of different passwords that must be used before a password may be re-used.)**	**Users must not reuse their previous twenty-four (24) passwords.**	***Same as field at left***	***Same as field at left***	**N/A**	**N/A**

Unauthorized Passwords	• **Passphrases/Passwords must not match or resemble:**
	  • **the word "password"**
	  • **the user's first or last name, or log-in name.**
	  • **the name of the system.**
	  • **dictionary words**
	• **Default passwords must be changed immediately after signing on.**
		Same as field at left	***Same as field at left***	***Same as field at left***	***Same as field at left***

Disabling accounts of High-Risk Individuals	• **Accounts can be directed to be disabled by CIO/CISO/ED ISSM/ISSO in reference to a security incident (reference**	***Same as field at left***	***Same as field at left***	***Same as field at left***	***Same as field at left***

	ED's Incident Response Process) • **If automated disabling capability is unavailable, manual methods must be implemented and documented in the System Security Plan (SSP). ISSOs are responsible for disabling inactive accounts.**				
Disabling Inactive Accounts	• **Accounts must be disabled after 90 days of inactivity.** • **If no automated capability is available, manual methods must be implemented and documented in the System Security Plan (SSP). ISSOs are responsible for disabling inactive accounts if the system cannot do so automatically.** • **This stage of disabling does NOT require the users to start the provisioning process from the beginning, but rather requires an admin to re-enable the account.**	***Same as field at left***	***Same as field at left***	**N/A**	**N/A**
Deactivating Inactive accounts	• **Accounts with no activity after 365 days must be**				

	deactivated. This requires the users to start the provisioning process from the beginning.	*Same as field at left	*Same as field at left	*Same as field at left	*Same as field at left
Account Deletion	• Accounts must be deleted in accordance with NARA General Records Schedule (GRS) 3.2 Information Systems Security Records OR the system retention schedule.	*Same as field at left	*Same as field at left	*Same as field at left	*Same as field at left
Verification	• Systems must automatically verify passwords.	*Same as field at left	*Same as field at left	N/A	N/A
Default Passwords	• Default passwords must be changed immediately upon sign-on.	*Same as field at left	*Same as field at left	N/A	N/A
Distribution of Passwords	• Passwords must not be sent via physical mail • User IDs and passwords must never be distributed in the same email. • For other than one-time use, passwords can only be sent to users via: - An encrypted FIPS 140-2 compliant Zip file - Text message - Voice transmission	*Same as field at left	*Same as field at left	N/A	N/A

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)