COMPLIANCE COMPONENT

DEFINITION	
Name	Password Controls
Description	A password is a secret string of alpha numeric characters that an individual uses to authenticate their identity. Password Controls are measures to protect information technology systems of value to the agency.
Rationale	A login ID with a password is the most common method of authenticating users to a system or application, and often the only security control employed. For systems that rely upon password protection, system administrators shall institute strong password controls, and users shall be responsible for creating strong passwords and keeping them secret.
Benefits	• Password controls provide a method to authenticate authorized users. • Password controls reduce the threat of password compromise as an avenue of attack on computer resources. • Password controls help prevent unauthorized persons from entering IT systems. • Password controls provide user accountability.

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Technical Controls
Specify the Technology Area Name	Identification and Authentication
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	**Password Control Guidelines** Systems that do not support external identification and authentication via an application-programming interface, or do not natively support the minimum password controls outlined in these guidelines, shall be upgraded, replaced, or reviewed by the ARC variance process. **General Password Requirements** • All IT systems and applications shall utilize, as a minimum form of security, a unique user identifier and a secret password as a means of authentication. • Network devices (routers, firewalls, access control servers, etc.) shall be password protected.

- Default administrative passwords must be changed on all hardware or software upon installation.
- Passwords shall not be hard coded into IT systems or applications.
- Passwords issued or reissued by systems or administrators shall be reset and uniquely defined by each user upon next login.
- Proof of identity shall be presented to the password reset administrator or system for user password resets, such as photo ID, supervisor verification, call back to an office supplied phone number and/or communication of a shared secret.
    - Note: Password reset administrators may reserve the right to refuse a password reset.
- Password resets or changes shall be promptly confirmed with the user. The confirmation method is at the discretion of each agency (e.g., phone, e-mail, registered mail, etc.).
- Passwords shall be changed after a system compromise or after the threat of a system compromise, such as the termination of a system administrator, security level change, etc.
- Users shall promptly change all passwords if they suspect or know other parties received the passwords.

Password Composition Requirements

Passwords are made up of various alpha numeric characters, which can be broken down into four character groups. These are uppercase alphabetic, lowercase alphabetic, numeric, and special characters. Increasing the length and complexity of passwords increases the time necessary to crack passwords exponentially.

- Passwords for all systems are subject to the following password composition rules:
    - Passwords shall contain characters from at least three of the following four categories:
        - English Uppercase Alphabetic (A - Z)
        - English Lowercase Alphabetic (a - z)
        - Numeric Base-ten digits (0 – 9)
        - Special characters (e.g., exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], asterisk [*], etc.)
    - Passwords are not to be your name, address, date of birth, username, nickname, or any term that could be easily guessed.
    - Passwords are not to be related to the job or personal life, e.g., not a license plate number, spouse's name, telephone number, etc.
    - Passwords are not to be dictionary words from any language or proper names, places or slang.
    - Passwords may not contain all or part (3 or more sequential characters) of the user's account or login name.
    - Passwords shall not contain characters that do not change combined with characters that predictably change when changing passwords upon expiration. For example, users may not choose passwords like "x345JAN" in January, "x345FEB" in February, etc., or identical or substantially similar to passwords the user previously chose.

Password Lifetime Requirements

The purpose for requiring password lifetime restrictions is to prevent users from using their favorite password until it expires, and changing their password more times than the system remembers, and cycling back to their

favorite password, thus circumventing the system.

- Passwords for all systems are subject to the following password aging and history rules:
    - Password age shall not exceed 60 days. However, passwords should be changed on a more frequent basis commensurate with the sensitivity, criticality and value of the information it protects.
    - Administrator password age shall not exceed 60 days.
    - Any default or initial password issued by a security administrator shall be valid only for the user's first logon.
    - Password history files should contain, at a minimum, the last 24 passwords particular to a logon ID to ensure that users do not cycle through regular passwords.
    - Any password reset must be changed by the user within 24 hours.

Password Length Requirements

An 8-character password made up of only lowercase characters has 26^8 possible passwords. An 8 character password made up of uppercase, lowercase, and special characters (on a standard 104 key keyboard) has 95 possible keys (excluding control characters) that make for 95^8 possible password combinations.

- All passwords shall be at least 8 characters in length, except within legacy systems that cannot support an 8 character password.
- Passwords that do not comply with the frequency portion of the Password Lifetime Requirements above, such as system service passwords, shall be at least 15 characters in length.

Password Source Requirements

- Only end-users or automated processes shall generate passwords.

Password Ownership Requirements

- Passwords for all systems are subject to the following password ownership rules:
    - Users shall not disclose their password to anyone.
    - Passwords should not be spoken, written, e-mailed, hinted at, shared, or in any way disclosed to anyone other than the user involved.
    - User-initiated password changes shall be supported on enterprise networks and systems.

Password Storage Requirements

- Passwords for all State IT systems are subject to the following password storage rules:
    - Users shall not record their passwords unless they have an approved secure method of storing them, such as an approved AES 256bit encrypted password manager.
    - Passwords are not to be displayed or concealed at the user's workspace.
    - Passwords shall not be stored in communications programs or Internet browsers such as auto fill fields.
    - Passwords stored and transmitted over open networks must be encrypted. For example, unencrypted FTP transmissions containing passwords are not acceptable.

Password Entry Requirements

In order to combat brute force and dictionary attacks, password entry requirements

	are established to disable an account after a specified number of failed logins occurs during a defined period of time. That account will remain locked out for a defined period of time. Enabling lockout policies make these attacks mathematically infeasible.
	
	• After a maximum of three invalid password or unsuccessful access attempts, one of the following actions shall be enforced:
	  ○ Disable or revoke the account until intervention by a system administrator.
	  ○ Suspend the account for at least 30 minutes.
	  ○ Disconnect communication service for external network connection.		

Document Source Reference #	NIST SP 800-63B		
Compliance Sources			
Name	NIST SP 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management	*Website*	https://csrc.nist.gov/publications/detail/sp/800-63b/final
Contact Information	inquiries@nist.gov		
Name	Publication 1075 (Rev. 9-2016) - Internal Revenue Service	*Website*	http://www.irs.gov/pub/irs-pdf/p1075.pdf
Contact Information			
Name	Missouri Revised Statutes Chapter 569 section 569.095	*Website*	http://moga.mo.gov
Contact Information			
KEYWORDS			
List Keywords	Complexity, access cards, smart cards, tokens, biometrics, user name, user ID, PIN, logon ID, lost, authentication, system, forgotten, reset, memorized secret, password		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Sunset Date			
CURRENT STATUS			
Provide the Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	02-13-2003	*Date Approved / Rejected*	05/16/2019
Reason for Rejection			
Last Date Reviewed	05/09/2019	*Last Date Updated*	02/23/2022
Reason for Update	Vitality		