



COMPLIANCE COMPONENT

DEFINITION	
<i>Name</i>	Password Controls
<i>Description</i>	<p>A password is a sequence of characters obtained by a selection or generation process from a set of acceptable controls.</p> <p>Password Controls are measures to protect information technology systems of value to the agency.</p>
<i>Rationale</i>	<p>A login ID with a secret password is the most common method of authenticating users to a system or application, and often the only technical control employed.</p> <p>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.</p>
<i>Benefits</i>	<ul style="list-style-type: none"> • Password controls provide a method to authenticate authorized users. • Passwords, if not handled correctly, can be the weakest link in the enterprise. • 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	
<i>Specify the Domain Name</i>	Security
<i>Specify the Discipline Name</i>	Technical Controls
<i>Specify the Technology Area Name</i>	Identification and Authentication
<i>Specify the Product Component Name</i>	
COMPLIANCE COMPONENT TYPE	
<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	
COMPLIANCE DETAIL	
<i>State the Guideline, Standard or Legislation</i>	<p><u>Password Control Guidelines</u></p> <p>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.</p> <p><u>General Password Requirements</u></p> <ul style="list-style-type: none"> • All IT systems and applications which access private or confidential information 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.
- 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 or knowledge 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 unauthorized parties received the passwords or they have shared it in the course of getting help with a problem.
- Restricted public access systems or machines that have no access to critical State of Missouri systems or data are exemptions to State password controls.

Password Composition Requirements

Passwords are made up of various characters, which can be broken down into four character groups. These are uppercase alphabetic, lowercase alphabetic, numeric, and special characters. Increasing the 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 90 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 session.
 - 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 14 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.
 - No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known 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:
 - Personnel shall not record their passwords unless they have a secure method of storing them, such as saving them in an encrypted file or storing them in a locked safe.
 - 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.

	<p><u>Password Entry Requirements</u> One method of gaining access to a computer system is to continuously access systems, using common account names, and different passwords until one works. Dictionary attacks use lists of common words as passwords in attempts to logon to a system. They are often successful against weak passwords. Brute force attacks attempt to use every possible character combination as a password, and will always be successful given enough time.</p> <p>In order to combat these 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.</p> <ul style="list-style-type: none"> • After a maximum of five invalid password or unsuccessful access attempts, one of the following actions shall be enforced: <ul style="list-style-type: none"> ○ 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. <p><u>Password Auditing Requirements</u></p> <ul style="list-style-type: none"> • An authorized system administrator shall audit all passwords to ensure compliance with password guidelines. 		
<i>Document Source Reference #</i>	NIST SP 800-18 draft		
Compliance Sources			
<i>Name</i>	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	<i>Website</i>	http://csrc.nist.gov/
<i>Contact Information</i>	inquiries@nist.gov		
<i>Name</i>		<i>Website</i>	
<i>Contact Information</i>			
<i>Name</i>	Missouri Revised Statutes Chapter 569 section 569.095	<i>Website</i>	http://moga.mo.gov
<i>Contact Information</i>			
KEYWORDS			
<i>List Keywords</i>	Passwords, password controls, digital signatures, access cards, smart cards, tokens, biometrics, user name, user ID, PIN, logon ID, dial-up, lost, forgotten		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i>	<input checked="" type="checkbox"/> <i>Current</i>	<input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>
<i>Sunset Date</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i>	<input type="checkbox"/> <i>Under Review</i>	<input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>

AUDIT TRAIL

<i>Creation Date</i>	02-13-2003	<i>Date Approved / Rejected</i>	03-24-2003
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	09-28-2011
<i>Reason for Update</i>	Vitality		