

CSF Controls: 01.r Password Management System

General Information

Control Reference:	01.r Password Management System
Control Specification:	Systems for managing passwords shall be interactive and shall ensure quality passwords.
Control Objective:	01.0 - Access Control 01.05 Operating System Access Control

Level 1 Implementation Requirement

Level 1 Organizational Factors:	None
Level 1 Regulatory Factors:	None
Level 1 System Factors:	Processing PHI: No – AND – Accessible from the Internet: No Number of Users: < 500 Exchanges Data with a Business Partner: No Third Party Support: No Publicly Accessible: No
Level 1 Implementation:	Refer to Sections 1.b and 1.f for a full list of password controls. In addition, a password management system shall be implemented to: <ol style="list-style-type: none"> 1. require the use of individual user IDs and passwords to maintain accountability; 2. allow users to select and change their own passwords and include a confirmation procedure to allow for input errors; 3. force users to change temporary passwords at the first log-on (see 1.b); 4. not display passwords on the screen when being entered; and 5. always change vendor-supplied defaults before installing a system on the network including passwords, simple network management protocol (SNMP) community strings and the elimination of unnecessary accounts.
Level 1 Control Audit Procedure:	Examine: <ol style="list-style-type: none"> 1. The policy and procedures for password management to ensure the allocation and enforcement of passwords is defined and controlled. Interview: <ol style="list-style-type: none"> 1. Select organization personnel to ensure IDs are linked to individual responsibility. 2. Select organization personnel to ensure temporary passwords must be changed at the first log-on. Test: <ol style="list-style-type: none"> 1. The operating systems on critical systems to validate that passwords are

Consistency in audit procedures allows apples-to-apples comparisons and improves the secure exchange of data throughout the information's lifecycle.

	not displayed on the screen when being entered.
Level 1 Control Standard Mapping:	<ul style="list-style-type: none"> HIPAA § 164.308 (a)(5)(ii)(D)

Level 1 Alternate Controls

<u>Control Name</u>	<u>Control ID</u>	<u>Control Type</u>	<u>Control Description</u>
Algorithmic and View-Based Access Controls	CA-4859	Compensating	Systems shall use algorithmic and view-based access controls implemented by operating systems, security subsystems, or database management systems (e.g., file attributes, access control lists, security rules, object-oriented security labels, database sub-schemas) to control access to data.

Reference mapping between the CSF controls and associated authorized Alternate Controls available for all organizations to use.

Level 2 Implementation Requirement

Level 2 Organizational Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance Subject to Federal Government Compliance
Level 2 System Factors:	Processing PHI: Yes – AND – Accessible from the Internet: Yes Number of Users: >500 Exchanges Data with a Business Partner: Yes Third Party Support: Yes Publicly Accessible: Yes
Level 2 Implementation:	Level 1 plus: Refer to Sections 1.b and 1.f for a full list of password controls. The password management system shall: <ol style="list-style-type: none"> store and transmit passwords in protected (e.g. encrypted or hashed) form; store password files separately from application system data; enforce a choice of quality passwords (see 01.b); enforce password changes (see 01.b); and maintain a record of previous user passwords and prevent re-use (see 01.b)
Level 2 Control Audit Procedure:	Examine: <ol style="list-style-type: none"> The policy and procedures for password management to ensure the allocation and enforcement of passwords is defined and controlled. Interview: <ol style="list-style-type: none"> Select organization personnel responsible for information security to verify that vendor-supplied defaults are always changed before installing a system on the network.

Scales according to type, size and complexity of the organization as determined by a predefined formula.

Follows a risk-based approach to allow organizations to identify the appropriate level of controls. This includes multiple levels of Implementation Requirements as determined by a risk assessment.

	<p>Test:</p> <ol style="list-style-type: none"> 1. The operating systems on critical systems using test ID's or accounts to validate that the selection of passwords is in accordance with the organization's policies (e.g. strong passwords must be chosen). 2. The operating systems on critical systems to validate that any vendor-supplied default passwords have been changed.
Level 2 Control Standard Mapping:	<ul style="list-style-type: none"> • ISO/IEC 27002-2005 11.5.3 • ISO 27799-2008 7.8.4 • NIST SP800-53 R2 IA-5 • PCI DSS v1.2 2.1.1 • PCI DSS v1.2 8.4 • PCI DSS v1.2 8.5 • PCI DSS v1.2 8.5.8 • PCI DSS v1.2 8.5.9 • PCI DSS v1.2 8.5.10 • PCI DSS v1.2 8.5.11 • PCI DSS v1.2 8.5.12 <div style="border: 1px solid black; border-radius: 15px; padding: 10px; margin-top: 10px; background-color: #800000; color: white; text-align: center;"> <p><i>Leverages existing globally and nationally recognized standards to expand on the implementation requirements of the framework and to avoid introducing additional redundancy and ambiguity into the industry</i></p> </div>

Level 2 Alternate Controls

<u>Control Name</u>	<u>Control ID</u>	<u>Control Type</u>	<u>Control Description</u>
Cryptography for User Authentication	CA-5117	Compensating	Systems shall use cryptography or cryptographic exchange to authenticate user access

Level 3 Implementation Requirement

Level 3 Organizational Factors:	None
Level 3 Regulatory Factors:	None
Level 3 System Factors:	None
Level 3 Implementation:	No additional requirements
Level 3 Control Audit Procedure:	

Level 3 Alternate Controls

<u>Control Name</u>	<u>Control ID</u>	<u>Control Type</u>	<u>Control Description</u>
No records specified.			

Standards Mapping

References:

21 CFR Part 11

- Subpart A – General Provisions
 - 13.3 Definitions
 - 11.3 (a) Sec 201 Definitions
 - 11.3 (b) Additional Definitions
- Subpart B – Electronic Records
 - 11.30 Controls for Open Systems
 - 11.30 (a) Controls for Open Systems
 - 11.50 Signature Manifestations
 - 11.50 (b) Controls on Electronic Signature Content
- Subpart C - Electronic Signatures
 - 11.100 General Requirements
 - 11.100 (a) Electronic Signature Uniqueness
 - 11.100 (b) Certification of Electronic Signatures
 - 11.100 (c) Legality of Electronic Signatures
 - 11.200 Electronic Signature Components and Controls
 - 11.200 (a) Non-biometric Signatures
 - 11.200 (b) Biometric Signatures
- HIPAA (August, 1996)
 - E. Administrative Safeguard (164.308)
 - Security Awareness and Training
 - (a)(5)(ii)(D) Password management (Addressable)
- ISO 27799:2008
 - 07.0 Healthcare implications of ISO/IEC 27002
 - 07.08 Access control
 - 07.8.4 Network access control and operating system access control
- ISO/IEC 27001:2005(E)
 - A.11.0 Access Control
 - A.11.05 Operating system access control
 - A.11.05.03 Password management system
- ISO/IEC 27002:2005(E)
 - 11.0 Access Control
 - 11.05 Operating system access control
 - 11.05.03 Password management system
- NIST SP 800-53 (February, 2005) and SP 800-26 (April, 2005)
Technical

Identification and Authentication

IA-05 Authenticator Management

PCI Data Security v1.2 (October 2008)

01 Build and Maintain a Secure Network (v1.2)

02 Do not use vendor-supplied defaults for system passwords and other security parameters (v1.2)

02.01 Vendor-Supplied Defaults (v1.2)

04 Implement Strong Access Control Measures (v1.2)

08 Assign a unique ID to each person with computer access (v1.2)

08.04 Password Transmission and Storage (v1.2)

08.05 Non-Consumer Password Management and User Authentication (v1.2)

Other Information

Other Information:

Passwords are one of the principal means of validating a user's authority to access a computer service. Some applications require user passwords to be assigned by an independent authority; in such cases, points b), d) and e) of the above guidance do not apply. In most cases, the passwords are selected and maintained by users.