Rule 4-004K Payment Card Industry (PCI) Access Management (proposed)

01.1 Purpose

01.2 Scope

The Access Management Rule applies to all information systems, resources and networks connected to the University of Utah ("University")’s network.

01.3 Rule Statement

01.4 User Enrollment and Authorization

01.4.01 User Enrollment Process

For all University employees, contractors or service providers that require access to University information systems, resources and networks, a [User Access Request] form shall be completed by [an authorized University employee] and forwarded to [University Information Technology ("UIT")] for review and approval. The User Enrollment Request process can be initiated by contacting the Help Desk [Ref: CS509, PCI, HIPAA]

The University's enrollment process shall be used to establish a user's identity and anticipated business needs to information, systems and resources prior to assigning a unique user identification (User ID).

01.4.02 User Registration

University employees, contractors and service providers that have been assigned a valid University Network ID (UNID), may request access to specific University applications or information resources through their respective manager/sponsor. This request shall be approved and signed by the requestor's immediate manager and forwarded to [UIT or ITS] Help Desk for processing. [UIT or ITS] is then responsible for forwarding the completed form to the appropriate information owner for final approval. [Ref: CS281, PCI, HIPAA]

A [User Access Request] shall be completed by a user's manager for requested modification to a user's access privileges. [Ref: CS280, PCI, HIPAA]

Information owners shall be responsible for reviewing and approving all requests for access to information resources and applications for which they have been assigned responsibility. Resource administrators shall be responsible for granting the level of access that has been approved by the information owner.
All [User Access Requests] shall be retained for a period of at least two (2) years and contain the classification of Restricted.
01.4.03 Review of User Access Privileges

Access privileges granted to general users shall be reviewed by information owners every six (6) months to determine if access rights are commensurate to the user's job duties. Evidence of account and privilege reviews shall be maintained for a period of twelve (12) months. [Ref: CS282]

Access privileges granted to privileged users shall be reviewed by the information owner at least every three (3) months to ensure the privileged access level is still valid. [Ref: CS283]

Managers shall be responsible for reporting changes in user duties or employment status for all employees under their supervision to the Human Resources department. The Human Resources department shall be responsible for reporting changes to information owners responsible for the information resources to which the involved user has access. Resource administrators shall promptly revoke all unnecessary access privileges. [Ref: CS284, PCI, HIPAA]

Information owners shall promptly report all changes in user duties or employment status to the resource administrator responsible for the User IDs associated with the involved personnel. Resource administrators shall promptly revoke all unnecessary access privileges. [Ref: CS285, PCI, HIPAA]

01.4.04 Access Management Systems

The University's access management systems shall provide effective mechanisms to ensure the University's password composition and usage policies are followed. [Ref: CS286, PCI, HIPAA]

[Rules] All of the University’s access management systems shall:

- Enforce the use of individual passwords to maintain accountability
- Allow users to select and change their own passwords
- Enforce alphanumeric password composition rules
- Force users to change temporary passwords at first login
- Require re-authentication prior to permitting a user to re-access an information resource after a period of inactivity
- Maintain a record of previous user passwords to prevent re-use
- Not provide specific feedback to the user if any portion of the login information is entered incorrectly
- Only indicate login failure after both the identifier and authentication information have been entered
- Display the number of unsuccessful login attempts made, since the last time the user successfully logged in
• Not display or allow printing of passwords on the screen while being entered
• Encrypt and store password files separately from system’s data
• Lock, disable or delete vendor accounts after product installation
• Not display system or application identifiers until the login process has been completed
• Not provide help messages during the login process that would aid an unauthorized user
• Not allow users to distribute passwords

1.5 Identification

01.5.01 User IDs

All users with access to the University's information systems, resources and networks shall use a UNID that has been specifically assigned to them. [Ref: CS287, PCI, HIPAA]

UNIDs shall be unique across all systems and forever connected with the single user to whom it has been assigned. To minimize the risk that dormant access permissions are accidentally inherited by a new user, there shall be no re-use of any UNIDs. [Ref: CS288, PCI, HIPAA]

UNIDs shall not be utilized by anyone except the individual to whom the IDs have been issued. Users shall be responsible for all activity performed with their personal UNIDs. [Ref: CS289]

Users shall not perform any activities with UNIDs belonging to others. [Ref: CS290]

01.5.02 Shared / Group IDs

Group, generic, or shared IDs are not permitted unless permission has been granted by the CISO. [Ref: CS292, PCI, HIPAA]

01.5.03 Default User IDs and Passwords

Default parameters, such as password length, composition, change schedules and other controls based on the account management standards, shall be set when creating new user accounts. These parameters shall be enforced either through the access management system or, if necessary, assigned to individual accounts in accordance with University standards [Ref: CS209]

All default, pre-set, or temporary passwords and accounts assigned internally shall be set to a unique value per user and changed immediately after first use. Vendor-supplied defaults shall be changed during installation of third-party software on the network. Additionally, all third-party software that comes with demo and/or sample applications shall be removed or disabled where applicable. [Ref: CS311]
[Rules] The following vendor-supplied defaults shall be changed:

- Passwords
- Elimination of unnecessary accounts / UNIDs (e.g., guest)
- Scripts, drivers, features, subsystems, file systems, and unnecessary web servers
- Simple Network Management Protocol [SNMP] community strings
- Wireless Equivalent Privacy (WEP) keys
- Service Set Identifier (SSID)
- Disabling of SSID broadcasts
- Enabling of Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.

01.5.04 Temporary User IDs

Temporary User IDs shall expire no more than ninety (90) days from the date of issuance [Ref: CS294, PCI]

Re-issuance of expired temporary UNIDs shall be re-approved by the information owner if a time extension is required. [Ref: CS295]

01.5.05 Group Membership

The ability to change group membership shall be restricted to authorized administrators. [Ref: CS302, PCI]

1.6 Authentication

1.6.01 Access Control Features

Access to all operating systems, information systems resources and networks shall be controlled by using unique UNIDs and one of the following authentication methods: passwords, token devices or biometrics. [Ref: CS296, PCI, HIPAA]

Users shall not be allowed to have a password that is the same as their User ID. User IDs and passwords contain a classification of [Restricted].

Access control features shall be provided within a separate software product or be embedded into features of the operating system to ensure that users have access only to the data and functions required in performing their duties [Ref: CS297, PCI, HIPAA]
Systems identified to be Sensitive or Restricted, as determined by the risk assessment, shall use additional authentication techniques in addition to User ID and password combinations (e.g., biometrics, cryptographic means, smart cards or tokens). [Ref: CS857, PCI]

**01.6.02 Password Length and Composition**

Password standards for length and composition shall be defined and enforced through the access management system. [Ref: CS299, PCI]

[Rules] Password shall be a minimum of eight (8) characters and contain at least two (2) of the following four (4) classes:

- English upper case letters (e.g., A, B, C, ...Z)
- English lower case letters (e.g., a, b, c, ...z)
- Westernized Arabic numerals (e.g., 1, 1, 2, ...9)
- Non-alphanumeric (""special characters) (e.g., ?,!,%,$,#, etc.)

Users shall choose easily remembered passwords that are, at the same time, difficult for unauthorized parties to guess. [Ref: CS300, PCI]

[Rules] The University recommends that users adhere to the following principles when creating passwords:

- Stringing several words together (the resulting passwords are also known as passphrases)
- Shifting a word up, down, left or right one row on the keyboard
- Bumping characters in a word a certain number of letters up or down the alphabet
- Transforming a regular word according to a specific method, such as making every other letter a number reflecting its position in the word
- Combining punctuation or numbers with a regular word
- Creating acronyms from words in a song, a poem or another known sequence of words
- Deliberately misspelling a word (but not a common misspelling)
- Combining a number of personal facts like birth dates and favorite colors
- Passwords shall not be associated with the University or the user (e.g., social security number, Employee ID number, address, numerical equivalent of name, family names, pet names, etc.)
• Passwords shall not contain words from dictionaries, movies, geographical locations or mythology. Passwords shall never be based upon month and year combinations such as "jan00" or "april2000".

01.6.03 Password Expiration

Passwords expiration standards shall be defined and enforced through the access management system. [Ref: CS301, PCI]

[Rules] The following password expiration rules shall be followed for PCI users, and administrators:

• Passwords for PCI users’ accounts shall have a maximum validity of [ninety (90)] days

• Password for privileged accounts (e.g., root, administrator, etc.) shall have maximum validity of [ninety (90)] days
  
  o Information Security strongly recommends these users utilize Multi-Factor Authentication

• Passwords for other user accounts, not mentioned above, shall not be required to expire

Users shall be provided the capability to change their password through secure protocols. The password change process shall include entry of the current password followed by entry of the new password twice. Both entries of the new password shall match in order to successfully complete a password change and the password change function shall verify the strength (e.g., length and composition) of the password prior to accepting the change. [Ref: CS304, PCI]

Where possible, a warning of password lifetime expiration shall be given to the user at least [five (5) days] and at every login during that period.

01.6.04 Password Storage

Passwords shall be stored using one way encryption or hashing (i.e., a password cannot be decrypted into clear text) to prevent their exposure to password cracking utilities. Passwords shall never be written down or stored on information systems in an unprotected form. Users shall not hard code any usernames/passwords in scripts or clear text files such as system shell scripts, batch jobs or word processing documents. [Ref: CS305]

01.6.05 One Time Use of Initial Passwords

When an account is created, it shall be assigned a random and secure password that is preset to expire upon login. The password can be generated by the system or by the creator of the account. The password assignments shall be unique to each user and the user shall be forced to change the password upon login. [Ref: CS308, PCI]

01.6.06 Password Resets
Passwords and UNIDs shall not be transmitted within the same electronic media (email) unless the message is encrypted. [Ref: CS309]

It shall be the responsibility of the access control authority, whether it is the information owner, resource administrator or help desk, to verify the identity and access level of the user requesting the reset, prior to the reset being performed. [Ref: CS310, PCI]

01.6.07 Inactive Accounts

PCI Systems:

User IDs not used for [ninety (90)] days shall be deactivated. User IDs not used for [one hundred fifty (150)] days shall be deleted and purged. Privileges and authorizations for the deleted User IDs shall also be revoked. All files owned by the User ID shall be identified and either archived or changed to a valid User ID. Records of all deleted User IDs shall be maintained for a period of [six (6)] months. [Ref: CS312, PCI]

All Other Systems:

User IDs not used for [three hundred sixty-five (365)] days shall be deactivated. User IDs not used for [five hundred (500)] days shall be deleted and purged. Privileges and authorizations for the deleted User IDs shall also be revoked. All files owned by the User ID shall be identified and either archived or changed to a valid User ID. Records of all deleted User IDs shall be maintained for a period of [six (6)] months.

01.6.08 Failed Login Attempts

For PCI Systems, and Systems with Restricted Data:

The maximum number of times a password can be attempted shall be [six (6)] times during a twenty-four (24) hour period. After the threshold has been violated, the user's password or User ID shall be either suspended until reset by a resource administrator or disabled for a period of not less than [thirty (30)] minutes. When a failed login attempt occurs, the user shall not be presented with any information regarding the User ID or password being entered incorrectly. It shall only state that the login was unsuccessful. [Ref: CS316, PCI]

Upon successful login, a message shall be displayed of the last successful login and the number of unsuccessful attempts to use the account. [Ref: CS453]

All Other Systems:

The maximum number of times a password can be attempted shall be [fifty (50)] times during a twenty-four (24) hour period. HSC and UUHC users of Apple Products may be granted this number of attempts pending a security exception review by Information Security.
01.6.09 Password History

Users shall not be able to construct passwords that are identical passwords they have previously employed in the last [five (5)] times they have changed their password. User selections for new passwords shall be checked against the history and rejected if there is a match. [Ref: CS317, PCI]

01.6.10 Display and Printing of Passwords and User IDs

The display and printing of passwords, UNIDs, and account numbers shall be masked, suppressed or otherwise obscured, such that unauthorized parties will not be able to observe or recover them. [Ref: CS318, PCI]

[Rules] Masking includes replacing passwords with a # or other character and using approved encryption methods for stored passwords:

- UNIDs shall not be shown unless there is a specific business use or it is required for end user interaction
- Passwords shall never be shown within an application or as clear text in storage
- For credit card systems, cardholder account numbers shall display a maximum of the first six and last four digits unless a specific need to see full credit card numbers is justified

Passwords shall not be transmitted in clear text. Passwords shall be encrypted for transmission. Password entry fields shall be masked from view and shall never be entered in clear text by a user. [Ref: CS319]

Password change mechanisms shall not pre-fill the User ID, unless strong authentication is being used. [Ref: CS320, PCI]

01.6.11 Automatic Logoff and Timeout

Users shall not leave any University information resource unattended that contains University information or is connected to a University network, and shall logoff or activate a screen saver program if the information resource in not used for a period of: [sixty (60)] minutes for general users and [fifteen (15)] minutes for administrative users. [Ref: CS468, PCI, HIPAA]

Information shall be enabled to automatically timeout the session after a maximum period of time. Re-establishment of the session shall take place only after the user has provided a valid password. [Ref: CS322, PCI]

For terminals or workstations in high-risk locations (e.g., public areas) or restricted systems (i.e., contains cardholder information), the time-out delay shall be set to a maximum of [fifteen (15)] minutes.

1.7 Privileged and Special Account Access
01.7.01 Special Privileges

All users that have access to privileged accounts shall have their own personal accounts for normal business use. Normal user accounts shall be used to access accounts that cannot be tracked to an individual, such as shared super user or privileged accounts. Shared super user or privileged accounts shall never be logged into directly if their usage cannot be tracked. Users with access to super user or privileged accounts shall use their normal account to log into information resources for day-to-day use. Administrators shall not use their privileged account for general use. [[Ref: CS325, PCI]]

All non-console administrative access shall be encrypted using technologies such as Secure Shell (SSH), Virtual Private Networks (VPN), Secure Socket Layer (SSL) or equivalents. This includes all remote sessions that are used for administrator access or privileged account access. [Ref: CS863, PCI]

01.7.02 Need to Know

Information and communication system privileges of all users, systems and independently operating programs such as agents, shall be restricted based on the need to know. This means that privileges shall not be extended unless a legitimate business need for such privileges exists. [Ref: CS329, PCI]

01.7.03 Least Privilege

The University's information owners, stewards, custodians and IT professionals/administrators shall only grant the minimum level of access required for users to successfully complete their job functions. [Ref: CS330, PCI]

01.7.04 System Utilities and Commands

Compilers or other system development tools shall not be installed in the production environment. All code shall be precompiled before moving into a production environment where applicable. If a compiler is necessary on a production machine, the access and execution rights shall be strictly controlled. [Ref: CS825, PCI]

01.8 Contacts

A. Policy Owner: Questions about this rule should be directed to the CISO, 801-213-3397
   IT_policy@utah.edu

B. Policy Officer: Only the CIO, 801-581-3100, has the authority to grant exceptions to this rule.

01.9 References

A. Policy 4-002: Information Resources Policy
B. Policy 4-004: University of Utah Information Security Policy
C. Data Classification Model
01.10 Policy Meta-Data

A. Policy Owner
B. Audience
C. Status
D. Published Date
E. Effective Date
F. Next Review Date

01.11 Revision History