Background

Strong authentication is an important aspect of computer security and is the front line of protection for user access to computerized information systems containing restricted data, identity information, financial information, or other electronic information. This policy is to ensure that all university employees (including contractors and vendors with access to university systems) take responsibility for using appropriate means for establishing positive identification when accessing university information systems.

Policy

IT@UC and University of Cincinnati data custodians (computer systems administrators), as defined within UC’s Data Protection policy, are responsible for ensuring that university information is protected from inappropriate disclosure. Such information may be “restricted”, “controlled” or “public” data (as defined in UC’s Data Protection Policy; see Related Links), electronic protected health information (ePHI), identity information, financial information, or other electronic information deemed sensitive. A key method of accomplishing this is the appropriate authentication of persons utilizing university computer systems. The policy for the University of Cincinnati computer system user authentication is as follows.

1. Authentication Requirement
   All users that access university computerized information systems containing or transmitting restricted data, including ePHI, must use some form of authentication which establishes their electronic identity and which can be used to audit their activities while accessing these systems. Allowed authentication forms include: an individual user ID coupled with a password or passphrase; biometric identification; public key infrastructure (PKI) key; secure certificate; password token; secure ID card (Smart Card); or combinations thereof. All university employees and non-employees using positive ID must make a reasonable effort to use such authentication when required.
2. **Authentication Responsibility**

Users are responsible for all activity performed with their authenticated identity and shall not permit others to perform any activity with their authenticated identity or perform any activity with the authenticated identity of another user. (See *Use of Information Technology Policy* in Related Links). Employees should not test or attempt to compromise internal controls unless specifically approved in advance and in writing by the IT@UC Office of Information Security or unless such activity is part of their normal job function for network or application system administration.

3. **Unique Identification Code (User ID)**

Every person receiving access to university information systems or services shall have a unique identification code (also known as a username, or user ID) assigned by IT@UC or the computer systems administrator.

4. **Group Sign-ons**

All university application systems containing restricted data and any other application system that could require any level of auditability shall not permit use of a group sign-on for access or system maintenance unless the group sign-on is to a computer that is used by more than one person and that computer can only access applications which require individual authentication.

5. **Re-use of User IDs**

Network user IDs may not be re-used except in the case of rehire or changed if the user’s name changes. Application system user IDs are generally not to be re-used. If it is necessary to re-use a user ID because of a system limitation, then a log indicating the period during which each usage of the user ID was in effect and who used it is to be kept by the department issuing the user IDs.

6. **Passwords**

Password Administration - Computer application systems shall have a password administration process. Best practices (as defined in *Appendix A – Password Best Practices*) shall be followed unless doing so is impractical or overly burdensome. All university employees are responsible for maintaining the confidentiality of protected information (i.e., restricted data). To this end, all electronic passwords are confidential.

Password Protection - Passwords should be protected from disclosure when stored electronically or on paper and should not be shared. Each password should be constructed such that it cannot be easily guessed or determined based on one’s knowledge of the user. Expired passwords should not be re-used immediately.
Users who suspect that their passwords have been inadvertently disclosed or compromised must immediately report the suspected compromise to IT@UC’s Office of Information Security and must change or reset all passwords in question.

7. **Passphrases**
   All of the rules that apply to passwords also apply to passphrases.

8. **Emergency Access**
   Systems deemed critical by the data trustee (see Roles and Responsibilities in the Data Protection Policy 9.1.1 in Related Links), should have a mechanism for emergency access, which will not compromise the security of mechanisms for normal access.

9. **Authentication Tokens**
   The university supports the use of two-factor authentication via a password challenge hardware token coupled with a user ID/password. This two-factor authentication is required for secure virtual private network (VPN) access to restricted data.

10. **Digital Certificate Authentication**
    The university supports the use of digital certificates issued by a certificate authority as a trusted form of authentication for client-server security and other forms of server-based security. Certificate authentication is performed via the public-key authentication method.

11. **Log-off**
    Users are required to log off of applications with access to restricted data immediately after finishing an access session. To ensure that this takes place, each application system shall, if possible, enact an automatic logoff or timeout that takes effect after a defined period of inactivity of the use of the application. Applications not having an automated logoff feature are to be documented (see Acceptance of Risk Policy 9.1.6 in Related Links), and use of a password-protected screen saver for the workstation shall be used in lieu of automatic logoff where possible.

12. **Policy Exceptions**
    Temporary exceptions to one or more sections of this policy or procedure may only be granted by the Office of Information Security (or organizational equivalent) or if required by law, licensure or other factors outside the control of the university. The exemption must be written, signed and kept by the Office of Information Security and must include the date of signing, the estimated end date of the exception(s) and the reason for the exemption (see Acceptance of Risk Policy 9.1.6). Employees that violate this policy will be subject to corrective action up to and including discharge as outlined in the Use of Information Technology Policy (see Related Links).
Related links:

- Acceptance of Risk Policy
- Appendix A - Best Practices
- Data Protection Policy
- Use of Information Technology Policy

Contact Information:

IT@UC Office of Information Security 513-558-ISEC
Email: infosec@uc.edu
UC Office of the CIO 513-556-2228

History:

Issued: 01/06/2008
Revised: 09/24/2014
1. Users should construct passwords with the following in mind:

   - Requiring passwords to contain both upper and lower case characters (e.g., a-z, A-Z).
   - Requiring passwords to consist of eight or more alphanumeric or special characters in a combination that is not obvious (e.g., no initials, repetitive patterns, etc.).
   - No more than 3 of any one character can be repeated in the password.
   - Ensuring passwords are not words in any language, slang, dialect, jargon, etc.
   - Ensuring passwords are not based on personal information (e.g., family names, birth dates, Social Security numbers, phone numbers, account numbers).
   - Ensuring passwords are not the combination of a set of characters that do not change, with a set of characters that predictably change (e.g., passwd1, passwd2, passwd3)
   - If using a passphrase, passphrases should be relatively long and contain a combination of upper and lowercase letters and numeric punctuation characters. The complexity standards that apply to passwords also apply to passphrases.
   - Changing all vendor-supplied default passwords immediately upon installation of the vendor’s product.
   - Setting the minimum password age to one day.

2. Automatic password saving or responding mechanisms should be disabled (such as those found in Internet Explorer.)

3. Passwords should only be transmitted in encrypted form.

4. An account should lock after five consecutive invalid login attempts, to prevent individuals from attempting to login to user accounts (i.e., user IDs) by guessing passwords.

5. A password should be changed immediately upon receipt unless the user established it his/herself and no one else can know it.

6. A password shall be changed at least every 90 days.

7. The same passwords for university accounts should never be used for other non-university access (e.g., personal bank accounts, charge account PIN, benefits, etc.).

8. University passwords should not be shared with anyone, including managers, administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

9. If someone demands that user reveal a password, they should be referred to this
10. Users should select application systems that:
   - Keep a password history of users’ six previous passwords to prevent individuals from reusing previously used passwords.
   - Prevent passwords from being visible on a screen, hard copy, or any other output devices (i.e., use non-display or overstrike fields).

11. If an account or password is suspected to have been compromised or misused, the incident should be reported to the IT@UC Office of Information Security and all passwords should be changed.

12. Users should be aware that password cracking may be performed periodically and randomly by the Office of Information Security or its delegates as approved by the Associate Director of Information Security. If a password is guessed or cracked during a scan, the user will be required to change it.

13. Users should contact the IT@UC Helpdesk or an authorized application system administrator to have a password reset. They should be prepared to answer questions that will authenticate their identity.

Do:

   - Take measures to safeguard passwords from discovery by others
   - Construct passwords that only the user can remember and that others cannot guess
   - Meet or exceed the organization’s policy requirements regarding passwords
   - Store passwords in files that are inaccessible to other users, in encrypted files, or in files that will otherwise be protected from disclosure.

Do not:

   - Reveal a password over the phone to ANYONE
   - Reveal a password in an email message
   - Reveal a password to a manager
   - Talk about a password in front of others
   - Hint at the format of a password (e.g., “my family name”)
   - Reveal a password on questionnaires or security forms
   - Share a password with family members
   - Reveal a password to co-workers while on vacation
   - Write down or otherwise record a readable password and store it near the access device to which it pertains
   - Allow a “new user” to use another user’s account for temporary access
   - Store passwords in logon scripts, software macros, terminal function keys, in computers without access control, or in locations where unauthorized users might discover or use them.