

Frequently Asked Questions: Passwords

Document Information	
Status	Published
Published	09/01/2008
Last Reviewed	10/17/2008
Last Updated	10/17/2008
Version	1.1

1. Why are passwords so important?

User authentication is one of the first lines of defense when protecting data from unauthorized access. It is the process by which a user validates that they are who they say they are. The combination of a username and a password is one of the most common forms of user authentication. Usernames are often readily available to an intruder (e.g. via a public directory). This makes the password critical to preventing unauthorized access. It is important that passwords are complex enough that they cannot be easily guessed by an intruder. It is also important that password complexity be supplemented with other controls such as a periodic password changes. See the [Guidelines for Password Management](#) for more information.

2. Why is the University asking me to change my password?

In an on-going effort to protect University resources, several changes are being, or have already been, made related to your passwords. Users of HRIS, Oracle Financials, SIS and PAS are now required to maintain a “strong” password on both their Andrew account and their application account(s). This measure helps prevent someone from quickly guessing your password through a variety of attack methods. Users will also be required to change their application account passwords every 90 days. Andrew account passwords will not have to be changed every 90 days.

While there is often much debate about the pros and cons of changing your password regularly, it is generally considered to be a best practice. Various industry standards bodies recommend this practice including the International Organization for Standardization (see ISO 27002 Section 11.3.1) and the IT Governance Institute (see COBIT Security Baseline). Some standards bodies, such as the Payment Card Industry Security Standards Council, require regular password changes. In this case, failure to do so can result in fines and the loss of credit card processing abilities for the University.

3. What is a strong password?

The Information Security Office has defined a “strong” password as followings:

A strong password should:

- Be at least 8 characters long
- Contain both upper and lowercase characters (e.g. A-Z, a-z)
- Contain at least one numerical character (e.g. 0-9)
- Contain at least one special character (e.g. ~!@#\$\$%^&*)

A strong password should NOT:

- Spell a word or a series of words that can be found in a standard dictionary
- Spell a word with a number added to the beginning or end
- Be based on personal information such as user id, family name, pet, birthday, etc.

See the [Guidelines for Password Management](#) for more information on maintaining a strong password.

4. Why were regular password changes not required in the past?

The University has recommended changing passwords on a regular basis for many years. However, evolving federal regulatory requirements and increased oversight into IT practices has created a need for more stringent enforcement of such practices. As a result, the University’s internal and external auditors have called for more proactive enforcement of industry best practices such as use of strong passwords and changing passwords at regular intervals.

5. Why has the University selected a 90 day interval for password changes?

Selecting an appropriate frequency for password changes is based on achieving some balance between the types of attacks used to compromise account passwords and the impact that password changes have on the user community. This frequency varies from one organization to another. Some organizations require monthly password changes, other quarterly and others biannually. Microsoft published a [best practice document](#) suggesting passwords should be changed every 42 days. This document was endorsed by various standards bodies such as the Center for Internet Security. The Payment Card Industry Security Standards Council adopted the 90 day interval in its [published standards](#). The University feels that requiring passwords to be changed every 90 days achieves a greater balance related to user impact than a shorter interval, while still maintaining its effectiveness as a security control.

6. Why do passwords have to be so complex?

Passwords must be complex in order to limit the possibility that they can be guessed. There are a variety of free tools available that would allow an attacker to rapidly guess passwords in an automated fashion. These tools make use of vast dictionaries, often in multiple languages. These tools also take into consideration common user practices such as capitalizing the first letter of a password or adding a numerical value to the end of a password. The password complexity requirements chosen by the University are considered a reasonable control against such automated attacks when also taking into consideration the impact on the user community of having an excessively complex password.

7. What users are required to have a “strong” password?

Users of the Human Resources Information System (HRIS), Oracle Financials, the Student Information System (SIS) and Property Accounting Services (PAS) are required to set a strong password for their Andrew account as well as accounts used to directly access these applications.

8. What users are required to change their password?

Users of the Human Resources Information System (HRIS), Oracle Financials, the Student Information System (SIS) and/or Property Accounting Services are required to change their application account password every 90 days.

9. What if I no longer need access to one or more of these applications?

If you no longer require access to one or more of the above referenced applications, please contact the appropriate group, as defined below, to request that your access be removed. If your access is removed from all referenced applications, you will not be required to change your application account password every 90 days nor will you be required to maintain a strong password. It is important to note that the Information Security Office encourages maintaining a strong password and periodically changing your password regardless of what systems you have access to.

Oracle Financials (OF)
Oracle Financials Help Desk
Email: orclhelp@andrew.cmu.edu
Phone: (412) 268-4666



Student Information System (SIS)
Contact: Russ Fetzko, Enrollment Systems Production Manager
Email: fetzko@andrew.cmu.edu
Phone: (412) 268-7646

Human Resources Information System (HRIS)
Contact: HR Systems Help Desk
Email: hrit@andrew.cmu.edu
Phone - (412) 268-3487

Property Accounting System (PAS)
Contact: Beth McShane, Manager Property Accounting
Email: em1y@andrew.cmu.edu
Phone: (412) 268-1640

10. What is the University doing to ease the burden of 90 day password changes?

The University is currently working on implementing a system that will allow the same user account and password to be used for multiple applications. Once implemented, users would only have to reset one password every 90 days instead of multiple passwords.

The University is also investigating the use of multi-factor authentication as an alternative to the more traditional username and password authentication scheme. There are three 'factors' related to authentication: something you know (e.g. a password), something you have (e.g. a key) and something you are (e.g. a fingerprint). If two or more factors are used to authenticate, then the loss or compromise of one factor is insufficient for an intruder to gain access. This could allow the University to ease restrictions on each individual factor (e.g. such as not requiring password changes every 90 days). Various multi-factor authentication techniques are being considered as part of the University's next generation of authentication solutions.