NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 114**
	Section: 100 General
	Page 1 of 2
	Responsible office: Comptroller
	Origination date: 01/01/2000
Subject: PeopleSoft Financials Security Access	Effective date: 01/01/2000
	Revision date: 01/25/2016

PURPOSE

To provide guidelines for secure access to PeopleSoft Financials.

SOURCE

University policy

BACKGROUND

User IDs identify the person authorized to use a particular system or application, and passwords are keys that unlock access to those applications and systems. Maintaining a secure computer environment relies on individual users safeguarding and keeping private their access information, including changing their passwords on a regular basis. If an individual obtains the password to a user's account, the user may be open to loss of data or unauthorized use of the account.

CMP 114: PeopleSoft Financials Security Access

Guidelines for Maintaining System Security

To obtain access to PeopleSoft Financials security, please refer to the ePASS web page.

To assist in maintaining PeopleSoft Financials security, follow the guidelines below:

1. Change passwords after receiving a new user ID.
2. Memorize the new password.
3. Choose a password that is a combination of letters and digits. Passwords must be at least 6 and not more than 14 characters in length. No special characters or spaces are allowed.
4. Never share the password with others.
5. Do not write the password on a paper or Post-it note and attach it to the computer or leave the written password on the desk, in a desk drawer, or on a calendar or desk pad.
6. Log off PeopleSoft before leaving the workstation.
7. Change passwords on a regular basis, e.g., every 42 days or sooner, especially when there is an attempt to access the account or if someone may have learned of the password.
8. If you fail to correctly input your password after three attempts, your account will be locked. For assistance, please contact the Help Desk at 3-1511.

NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 114**
	Section: 100 General
	Page 2 of 2
	Responsible office: Comptroller
	Origination date: 01/01/2000
Subject: PeopleSoft Financials Security Access	Effective date: 01/01/2000
	Revision date: 01/25/2016

CMP 114: PeopleSoft Financials Security Access

Choosing and Safeguarding Passwords

Passwords that have some connection to the user (e.g., names, addresses, telephone numbers, and initials) are the easiest to break. This type of information is public knowledge and should not be used to formulate a password. Common words should not be used for passwords since hackers have programs that automatically search through dictionaries trying each entry as a password. A good password is difficult to break, easy to remember, and long enough so that trying random combinations of letters will not uncover it.

Creativity is important in choosing a password. Combining the first letters from the words of a line in a favorite song along with a random number or letter is just one way to form a good password that is cryptic but easy to remember. Once the user has chosen a password, it is important to protect it. Do not write the password on paper or Post-it note kept near the workstation. Users should treat computer accounts and passwords as valuable commodities.

Changing Passwords

Passwords should be changed regularly. If there is any reason to believe that the user's password is no longer secret or if the user notices someone watching his or her fingers while logging on to the system, change the password at once.