User Password Creation	**6-004** **INFORMATION TECHNOLOGIES** **May 2013**

POLICY

1.01 Every person using computers, accessing servers, cloud services, local services or accounts used for university business must adhere to this policy. The technology equipment and the information stored and transmitted on the university network are property of the university and must be safeguarded.

1.02 A password is private information. Users must be required to follow good security practices in the selection and use of passwords. Passwords provide a means of validating a user's identity and thereby establish access rights to information processing facilities or services. Any use of a user id, the unique identifier associated with the person and used for university business, is the responsibility of the individual to whom the user id is assigned. Any use of files or services associated with a user id is also the responsibility of the individual to whom the user id is assigned.

1.03 Each individual is responsible for safeguarding passwords associated with their user id. Passwords must not be shared. It is against policy and in most cases the law, to use another individual's account or to share your credentials with another individual. Failure to conform to these restrictions may lead to the suspension of the user id or other action as provided by university policy or federal and/or state law. A supervisor may request access to an employee's information technology resources, through the CIS service desk, in emergency situations or when the employee is not on campus. This access can, in most cases, be done without compromising the employee's password and user id.

PROCEDURES

2.01 Each individual has the responsibility for creating and securing an acceptable password per this policy

A. Password Minimum Complexity:

1. The password must be 8-32 characters in length.

2. The password must not contain dictionary words.

3. The password must contain at least 1 upper case letter.

4. The password must contain at least 1 lower case letter.

5. The password must contain at least 1 number.

6. The password must not contain spaces.

7. The password must not be one of the last 4 passwords used.

8. The password may contain any of the following special characters:
   ~,!,@,#,$,^,*,(,),_,+,=,-,?,,,.

9. The password must not include the first, middle, or last name of the person issued the user id.

10. The password must not be information easily obtainable about an individual. This includes license plate, social security, telephone numbers, or street address.

11. Passwords should not be included in any automated log-on process.

12. Passwords should be created so as to be easily remembered.

13. Passwords should not be recorded except in a secure location.

B. Password Expiration and Reset

Passwords must be changed whenever there is a belief that the password has been compromised. In the event that a password is entrusted to CIS personnel to service a computer, troubleshoot a problem, or access is given to a supervisor in an emergency situation, the password should be reset when the issue is resolved. If a newly activated user id is assigned a temporary or default password, the temporary or default password must be changed at the first use. Passwords must be changed quarterly. Passwords may expire automatically on various time cycles depending on the system.