

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY
POLICY & PROCEDURES LETTER

User Password Creation

**6-004
INFORMATION
TECHNOLOGIES
July 2009**

POLICY

- 1.01 Every person using computers and accounts controlled by Computing & Information Services (CIS) will adhere to this policy. This policy is strongly recommended for all non-CIS systems administrators.
- 1.02 A password is private information. Any use of a userid (the unique identifier associated with the person and assigned by CIS) is the responsibility of the individual to whom the userid is assigned. Any use of files associated with a userid is also the responsibility of the individual to whom the userid is assigned.
- 1.03 Each individual is responsible for safeguarding passwords for their userid. Passwords must not be shared. It is against policy and, in most cases, the law to use another individual's account or file. Failure to conform to these restrictions may lead to the suspension of the userid or other action as provided by University Policy or Federal and/or State law.
- 1.04 Each individual has the responsibility for creating and securing an acceptable password per this policy
- A. Password Creation Recommendation:
1. The password must be at least six characters in length.
 2. The password must be a non-dictionary word.
 3. The password must contain characters from three of the following four categories:
 - English upper case characters (A...Z)
 - English Lower case characters (a...z)
 - Base 10 digits (0...9)
 - Nonalphanumeric (For example,!,\$,#,%)
 4. The password must be significantly different from previous passwords.
 5. The password must not contain all or part of the userid.

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY
POLICY & PROCEDURES LETTER

6. The password must not start or end with the initials of the person issued the userid.
7. The password must not include the first, middle, or last name of the person issued the userid.
8. The password must not be information easily obtainable about an individual. This includes license plate, social security, telephone numbers, or street address.

B. Password Expiration

Passwords should be changed whenever there is a belief that the password has been compromised. All newly activated userids are assigned a temporary password, which must be changed at the first use. Passwords should be changed quarterly. Some passwords may expire automatically on various time cycles.

Effective: March 7, 2003
Revised: October 2004
Revised: July 2009