

**POLICIES AND PROCEDURES  
OUACHITA TECHNICAL COLLEGE**

**SUBJECT AREA: Information Technology**

**POLICY/PROCEDURE: Passwords**

**DATE: 28 November 2006**

**NUMBER: 6.06**

**REVISION(S):**

**Passwords**

Campus electronic communications systems or services must identify users and authorize access by means of passwords or other secure authentication processes. When passwords are used, they must meet the **Minimum Password Complexity Standards** as described below. In addition, shared-access systems must enforce these standards whenever possible and appropriate and require that users change any pre-assigned passwords immediately upon initial access to the account.

All default passwords for access to network-accessible devices must be modified.

**Minimum Password Complexity Standards**

All passwords must meet the following complexity guidelines:

The password **MUST**:

- Contain eight characters **or more**
- Contain characters from **all** of the following **three** character classes:
  1. Alphabetic (e.g., a-z, A-Z)
  2. Numeric (i.e. 0-9)
  3. Punctuation and other characters (e.g., !@#\$%^&\*()\_+|~-=\`{ }[]: ";' < > ? , . /)

The password **MUST NOT** be:

- A derivative of the username
- A word found in a dictionary (English or foreign)
- A dictionary-word spelled backwards

A dictionary-word (forward or backwards) preceded and/or followed by any other single character (e.g., secret1, 1secret, secret?, secret!)

Passwords are used for various purposes at OTC. Some of the more common uses include: local accounts, web accounts, and email accounts. A weak (or absent) password is one of the most

common ways for an attacker to compromise your account; therefore, you should be aware of how to select strong passwords.

**Other Password Guidelines**

- Do not use an easily guessed password. Some examples of passwords that would be easy to guess:
  - Names of family, pets, friends, co-workers, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Passwords should never be written down or stored on-line.
- In general, a password should be as long as possible while still being easy-to-remember. One way to do this is create a password based on an easy-to-remember phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "Tmb1W>r~" or some other variation. NOTE: Do not use this example
- You should change your passwords on a regular basis, at least every six months. You should also change your password any time you suspect that your account has been compromised or tampered with and notify the IT department.

Try to use a different password for every system. At a minimum, do **NOT** use the same password for any of your Campus accounts that you use for a non-Campus service or third-party web site.

AUTHENTICATION (Signature):		COPP
_____	28 November, 2006	
President	(Date)	6.06