OAKLAND UNIVERSITY

Tuesday, July 15, 2003

New password guidelines implemented

*By **Jeff Samoray**, OU Web Writer*

To increase the security of Oakland University's computer networks, **University Technology Services** (UTS) implemented new password management guidelines beginning July 9. The guidelines, implemented to heighten security awareness and reflect best practice standards for all computer users, apply to all ADMNET and OPENNET accounts.

Individual user IDs and passwords are used to verify a user's identity and act as a unique key to system security. Network passwords should follow these guidelines:

- Passwords must have at least six characters.
- Characters should include upper and lower case letters.
- Characters should include Arabic numerals.
- A password should include at least one special character.
- Numbers and special characters should not be the first or last character in the password.
- Passwords should contain no more than two consecutive repeating characters (e.g. mm, 44, etc.).

Good examples of strong passwords include:

- hAp_py6ay
- h31L0_2u
- tIanIc

"These new password guidelines apply to anyone who logs on to the OU network," said Security Systems Analyst Chris Condie. "Using upper and lowercase letters helps make a password stronger and more difficult for someone using a password cracking program. If you are prompted to change your password, you have entered another one incorrectly, such as using five characters instead of six, a pop-up message will indicate what the problem may be. Users also can call the HelpDesk with any other concerns."

UTS suggests the following guidelines to ID/password utilization:

- To ensure confidentiality, do not share user IDs, birth dates, Social Security Numbers or other identifiers.
- Do not disclose your password to anyone or allow anyone to observe your password as you enter it.
- When selecting a password, avoid personal associations or ones that are simple or short.
- To further increase security, users will be required to change their passwords every 90 days and rotate between at least three different passwords. If your password is not changed within 90 days, your account will be locked.

After logging on, the network will attribute all activity to your user ID. It is a good policy to not leave your workstation without either locking your machine or logging off the network, even if only for a few minutes. Windows users also can utilize the standard screen saver that requires a password to be entered to regain access to your workstation.

For more information regarding password usage, visit the **University Technology Services** Web site. Further tips on effective password creation are available on the **Computerworld** Web site. Those needing assistance regarding passwords can contact the UTS HelpDesk at (248) 370-HELP (4357) or **help-desk@oakland.edu**.

SUMMARY
To increase the security of Oakland University's computer networks, University Technology Services implemented new password management guidelines beginning July 9. The guidelines, implemented to heighten security awareness and reflect best practice standards for all computer users, apply to all ADMNET and OPENNET accounts.

Created by CareTech Administrator (webservices@caretechsolutions.com) on Tuesday, July 15, 2003
Modified by CareTech Administrator (webservices@caretechsolutions.com) on Tuesday, July 15, 2003
Article Start Date: Wednesday, November 19, 2003