

<b>Policy #:</b>	<b>Title:</b>	<b>Effective Date:</b>
GEN-012	Password Policy	04/13/2009

**Policy Description**— To protect confidential information contained in The University of Findlay’s (UF) administrative and communication systems, account passwords will be subject to the following rules. Applied through the University’s Identity Management System, these rules will ensure everyone with a UFnet account uses a strong password.

1. Passwords must consist of eight or more characters.
2. Passwords must contain one or more of each of the following character types.
  - a. Uppercase characters from the English Alphabet (A-Z)
  - b. Lowercase characters from the English Alphabet (a-z)
  - c. Digits (0-9)
3. Passwords should be chosen using random characters and digits, and users are encouraged to include special characters. Users should avoid including proper words within their password.
4. Five invalid login attempts within one hour will lock that account for a period of one hour or until the password is reset. Passwords can be reset by self-service password reset or by contacting Technology Support Services (419-434-4357; or ext. 4357 on-campus).

---

**Definitions**—

*Strong Password*— A password containing a combination of letters and numbers (special characters are also encouraged) that is resistant to brute force attempts to guess the password.

*UFnet Account*— An account with a single username and password created by Information Technology Services that provides access to administrative, communication and educational technologies.

---

**Rationale for Policy**— Though many UFnet account holders may feel their password is not important because their individual data wouldn’t be valuable to others, access to UF technologies through a UFnet account username and password provides access to UF resources and may be used to further escalate privileges for unethical and/or illegal purposes. The aforementioned strong password rules are needed to prevent an attacker from using password cracking tools to obtain a password. These rules provide a key-space of 218,340,105,584,896 ( $62^8$ ) possible combinations for a minimally compliant password. Using current password cracking programs, an attacker making the maximum five guesses per hour against each of 10,000 accounts would require nearly 500,000 years to compromise the entire key-space, or 25 years to have a 50% probability of compromising a single account.

---

**Responsible Department/Person**— Information Technology Services/Information Technology Officer/Network Systems Manager

---

**Reference/Related Information**—

---

<b>Policy #:</b>	<b>Title:</b>	<b>Effective Date:</b>
GEN-012	Password Policy -- Page 2	04/13/2009

**Who should be notified about this policy—** All UFnet account holders

---

**Issue Date:** 02/01/2009

---

**Modification History—**