WASHINGTON STATE UNIVERSITY
EXECUTIVE POLICY MANUAL
Executive Policy #18
Approved December 2, 2005

Computer and Network User Identification and Password Policy

BACKGROUND

The discipline of information systems security is based on the notion of controlling access between system users and system resources in a shared networked environment. Controlling access generally relies upon establishing an identity (e.g., user ID) for each system user so that this information, in conjunction with some form of authentication (e.g., password), can be used as the basis for determining whether a user has the proper authorization to access a given resource. Computer user IDs and passwords are typically one of the weakest links in any security methodology. Information system security depends upon authentication information being kept secret. The proper use of user ID and password information is fundamental to information system security and is often the first line of defense users have against unauthorized access to network resources.

Also refer to:

> *Executive Policy* #4: Electronic Communication Policy: Policy on Electronic Publishing and Appropriate Use of Information Technology Resources
>
> *Executive Policy* #8: University Data Policies
>
> *Executive Policy* #16: University Network Policies

PURPOSE

This policy is intended to help promote a secure computing environment at Washington State University (WSU) by (1) establishing minimum user ID and password requirements for all WSU computer and network system users, (2) enabling WSU system administrators to set appropriate department/area user ID and password policies and procedures, and (3) to ensure that sound and secure user ID and password management practices are consistent University-wide.

SCOPE

This policy applies to all users of WSU owned and maintained systems and WSU provided IT services and resources. This includes, but is not limited to, WSU faculty, staff, students, associates, alumni, business partners and contractors.

Computer and Network User Identification and Password Policy

POLICY

1. User IDs shall be unique and assigned to an individual WSU computer and/or network system user. Shared computer and/or network system user accounts shall only be used when it is not operationally feasible to do otherwise, and the risk of using shared accounts is at an acceptable level.

2. It is the responsibility of everyone to keep his or her passwords secret. Passwords are considered confidential information and shall not be shared or transferred to others.

3. Passwords should not be written down. Where it is considered necessary to store passwords off-line, passwords shall be protected by some other level of security (e.g., Physical Security mechanism such as a locked safe or cabinet).

4. Where technically and operationally feasible, passwords shall not be electronically stored, cached, or transmitted in clear text.

5. The responsible administrative authority shall periodically review and remove or modify WSU computer and network system user accounts as appropriate or whenever the status of the user changes.

6. Passwords must be changeable by the user except in the extraordinary case of shared user IDs and passwords. In the case of shared user IDs and passwords, procedures must be in place to securely manage the shared user ID and password (e.g., password change and distribution).

7. Where technically and operationally feasible, minimum password requirements for WSU computer and network systems are as follows:

   - Passwords shall be a minimum of 8 characters in length for general users, and a minimum of 10 characters in length for users with elevated privileges (e.g, system and network administrators).

   - Passwords shall consist of at least one of each of the following character sets: letters, numbers, and special characters (i.e., !, @, #, $, %, &, *, +, ?). Sample password: 9u1!m@n!

   - When choosing passwords, users should avoid using their name, pet's name, relative's name or other common names, user ID, dictionary words (including words from foreign language dictionaries), birth date, phone number, address, or any other type of personal information or that which is easily derived from such information.

Computer and Network User Identification and Password Policy

POLICY (cont.)

- Passwords shall be changed at regular intervals, 180 days for general users and 90 days for users with elevated privileges.

- A password history file shall be implemented to discourage the reuse of recently used passwords. A password history of the three most recently used passwords shall be kept for general users and a password history of the six most recently used passwords shall be kept for users with elevated privilege.

- After 5 consecutive unsuccessful logon attempts, computer and network system user accounts will be locked out for a period of at least five minutes.

8. Authentication information stored on any University computer or network system shall be protected so the authentication information cannot be accessed by an unauthorized user or process.

9. Washington State University reserves the right to review and/or require change of any identification and/or authentication process for compliance with this policy.