

934 USE OF PASSWORDS POLICY

Policy 934 was approved by the ISU Board of Trustees on July 18, 2003.

934.1 Overview. Security for University-owned data systems and the information they contain is a primary concern. While a variety of means are used to achieve system and data security, the use of a username and password remain one of the most effective means of providing security for, and protecting access to, data. Stated in another way, passwords are the “keys” to a system. In order to ensure that proper use of password protection is implemented, it is necessary for the University to define a set of minimum standards for the use of passwords.

934.2 Definitions.

934.2.1 Password. Password means a protected/private string of alphanumeric characters used to authenticate an identity or to authorize access to data. A password is a group of characters used in conjunction with a username (or user ID) to achieve security by permitting access to data, information, or facilities that would be otherwise inaccessible.

934.2.2 Username. Username means the name or user ID assigned to each individual that identifies that individual to various systems and network resources.

934.3 Statement of Policy. Passwords should follow the generally accepted technology industry standard. Specifically a good password has the following qualities:

- (a) Has at least eight characters — the shorter the password, the generally easier it is to crack.
- (b) Is made up of characters, numbers, and symbols — Numbers and symbols hidden within letters (or vice versa) lengthens the possible number of options for a given password, which strengthens the overall password.
- (c) Is unique — Select passwords that are different than other passwords you may be using. If all of your passwords are the same or very similar, the magnitude of a security breach can be much greater.
- (d) Are not dictionary words — by using dictionary words as passwords, you are making it exponentially easier for your system to be cracked. Don't do it, and don't override authentication schemes that prevent the use of dictionary words to allow your users to do it.
- (e) Are not tied to your personal information — If you use passwords that are your birthday, spouse's name, or the make of your car, you are asking for trouble. Think about every password you use and determine whether or not someone who knows you could guess it. If there is even a slight chance they could, don't use that password.
- (f) Can be typed quickly — if your password is so complicated that you must hunt-and-peck for the characters each time you type it, prying eyes could easily watch your fingers and guess your password. At the very least, practice typing your password while alone to increase the speed in which you can type it.

(g) OIT shall have responsibility for all system level passwords. The passwords will be maintained in a central production database and shall be changed quarterly, at a minimum (passwords for IDs that have the capability to set security related items). IDs with system-level privileges must have different passwords from all other accounts owned by systems or network personnel that use the system-level accounts.

934.4 Responsibility for Protection of Password. Users will be responsible for the protection of their individual password(s). User level passwords must be changed each six months at a minimum. Passwords inserted in email, other electronic communication, or placed in a digital storage format must be encrypted. Passwords are not to be shared with anyone else. Users should use different passwords for ISU accounts versus those used for non-ISU accounts.

934.5 No Exceptions. There are no exceptions to this policy.

Last revised February 1, 2011.