



## **Password Policy**

### **1.0 Overview**

Passwords are used for various purposes at Plymouth State University. Some of the more common uses include: user-level accounts, web accounts, email accounts, screen saver protection, voicemail, server/system-level access, and network switch/router access.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Plymouth State University's system resources. As such, all Plymouth State University employees (including contractors and vendors with access to Plymouth State University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

### **2.0 Purpose**

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

### **3.0 Scope**

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Plymouth State University facility, has access to the Plymouth State University network, or stores any non-public Plymouth State University information.

### **4.0 Policy**

#### **4.1 General**

##### **A. User-Level Passwords**

- Passwords need to be a minimum of 8 characters and contain at least one uppercase character and one numeric character. They may not contain @ or ; (semicolon) or \$.
- Passwords (e.g., email, web, desktop computer, etc.) need to be changed upon the first login and at least every six months thereafter.
- Passwords shall not be inserted into email messages or other forms of electronic communication.

##### **B. Server/System-Level Passwords**

- All server/system-level passwords (e.g., root, sysadmin, application administration accounts, etc.) must be changed from vendor defaults and at least every six months thereafter.
- All server/system-level passwords must be a minimum of 8 characters and contain at least one uppercase letter and one numeric character.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv3).
- All server/system-level passwords must conform to the guidelines described below.

#### **4.2 Guidelines**

##### **A. General Password Construction Guidelines**



Everyone should be aware of how to select strong passwords. Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !#%^&\*()\_+|~-
- =\{}[]";'<>?,./) PSU passwords cannot contain the following characters: @ or ; or \$.
- Are at least eight alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.[The "not" and "never" points should be included under "weak passwords", above]
- Are not based on personal information, names of family, etc.
- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- Other examples...
  - We take your protection seriously, you should too = Wtyssus2
  - ITS is one of a kind, great = ITSi1oakgr8
  - CIO loves to ride bikes for fun = cio1trb4F

#### **B. Password Protection Standards**

All passwords are to be treated as sensitive, confidential Plymouth State University information. If an account or password is suspected to have been compromised, report the incident to ITS Security Officer and change all passwords.

Specifically, users should never:

- Reveal a password to ANYONE over the phone or in an email message
- Share a password with anyone, including family members, colleagues, administrative assistant or supervisors, even if going on vacation.
- If someone demands a password, refer them to this document or have them call the ITS Security Officer.
- Use the same password for Plymouth State University accounts as for other non-Plymouth State University access (e.g., personal ISP account, option trading, benefits, etc.)
- Use the "Remember Password" feature of applications (e.g., Zimbra, Outlook, etc.)
- Write passwords down and store them where they could be easily found in your office.
- Store passwords in a file on ANY computer system (including PDAs or similar devices) without encryption.

#### **C. Software Application Development Standards**

Software application developers must ensure their programs contain the following security precautions:

- Support authentication of individual users, not groups.
- Do not store passwords in clear text or in any easily reversible form.
- Provide a hierarchical role-based architecture that enables functions to be performed without sharing passwords between users.

#### **D. Use of Passwords for Remote Access**

Authorized users may remotely access Plymouth State University system resources via the university VPN. The user is responsible for ensuring that others within the remote environment are not able to learn his/her password during login to the university VPN.



## **5.0 Administration**

Violation of these guidelines constitutes unacceptable use of computer resources and may violate other University policies and/or state and federal laws. Suspected or known Password Policy violations should be reported to the Chief Information Officer (2443), Dean of Students (2260), and/or the Director of Human Resources (2551) who will process them in accordance with established University policies.

Violations may result in revocation of computer resource privileges, disciplinary action or legal action.

The maintenance, operation, and security of computing resources require responsible PSU personnel to monitor and access the system. To the extent possible in the electronic environment and in a public setting, a user's privacy will be preserved. Nevertheless, that privacy is subject to applicable University System of New Hampshire policies, state and federal laws, and the needs of the University to meet its administrative, business, and legal obligations.

## **6.0 Revision History**

06/02/08 ALB Policy created