Password Protection Policy

1. Overview
Passwords are an important aspect of computer security. A poorly chosen or shared password may result in unauthorized access and/or exploitation of the user or Rose State College's resources. All users, including contractors and vendors with access to Rose State College systems, are responsible for taking the appropriate steps, as outlined below, to secure their passwords.

2. Purpose
Rose State College provides access to network resources and use of application software that is licensed exclusively for use by current Rose State College students, faculty and staff. The purpose of this policy is to establish a standard for the protection of the passwords used to access these resources, and the frequency of which they should be changed.

3. 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 Rose State College facility, has internal or external access to the Rose State College networks, or stores any nonpublic Rose State College information.

4. Policy

4.1 Password Creation
4.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.
4.1.2 Users must not use the same password for Rose State College accounts as for other non-Rose State College access (for example, personal banking accounts, personal email, benefits, and so on).
4.1.3 Where possible, users should not use the same password for various Rose State College access needs.
4.1.4 User accounts that have system-level privileges granted through group memberships such as domain administrators must have a unique password from all other accounts held by that user to access system-level privileges.
4.1.5 Where Simple Network Management Protocol (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. SNMP community strings must meet password construction guidelines.

4.2 Password Change
4.2.1 All system-level passwords (for example, root, enable, administrator, local administrator, application administration accounts, and so on) should be changed on at least a quarterly basis.
4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) should be changed at least every six months. The recommended change interval is every four months.
4.2.3 Password cracking or guessing may be performed on a periodic or random basis by the IT Services Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

This document is reviewed annually. Last review date is DEC 2014
4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Rose State College information.
4.3.2 Passwords must not be inserted into email messages, texted or other forms of electronic communication.
4.3.3 Passwords should not be revealed over the phone.
4.3.4 Do not reveal a password on questionnaires or security forms.
4.3.5 Do not hint at the format of a password (for example, "my family name").
4.3.6 Do not share Rose State College passwords with anyone, including administrative assistants, secretaries, managers, co-workers, and family members.
4.3.7 Do not write passwords down and store them in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).
4.3.9 Any user suspecting that his/her password may have been compromised must report the incident to the IT Services department at Rose State College.
4.3.10 If IT Services suspects that a user’s password has been compromised without the user’s knowledge; IT Services may disable the account and reset the password without notice to the user until they have contacted the IT Services support team to have it re-enabled.

4.4 Application Development
Application developers must ensure that their programs contain the following security precautions:
4.4.1 Applications must support authentication of individual users, not groups.
4.4.2 Applications must not store passwords in clear text or in any easily reversible form.
4.4.3 Applications must not transmit passwords in clear text over the network.
4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Use of Passwords and Passphrases
4.5.1 Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:
"The*!?@*TrafficOnThe101Was*&#!#ThisMorning"
4.5.2 All of the rules above that apply to passwords apply to passphrases.

5. Policy Compliance
5.1 Compliance Measurement
5.1.1 The IT Services team will periodically verify compliance to this policy through various methods, including but not limited to, network scans of random or suspect PC’s, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner by onsite users of the campus networks.

5.2 Exceptions
5.2.1 Any exception to the policy must be approved by the IT Services Team.

5.3 Non-Compliance
5.3.1 Any employee found to have violated or is in violation of this policy may be subject to administrative or disciplinary action.

This document is reviewed annually. Last review date is DEC 2014
5.3.2 Any student found to have violated or is in violation of this policy may have their network account disabled restricting ALL access to Rose State College networked resources as well as external resources (such as email accounts and student enrollment thru the OASIS system).

This document is reviewed annually. Last review date is DEC 2014