General Password Guidelines – Last Amended September 2016

General

1. Except where technically not possible, all passwords should meet the following minimum standards
    - be at least eight alphanumeric characters long.
    - contain digits or punctuation characters as well as letters (e.g., 0-9, + ? . * ^ \$ ( ) [ ] { } / ~ ! \ @ # & = , -) NOTE: other special characters cannot be used in passwords for most Rhodes systems.
    - contain both upper and lower case characters (e.g., a-z, A-Z).
    - not be a word in any dictionary, language, slang, dialect, jargon, etc.
    - not be solely based on easily guessed personal information, birthdays, names of family members, pets, etc.
2. To help prevent identity theft, personal or fiscally useful information such as identity or credit card numbers should never be used as a user ID or a password.
3. All passwords are to be treated as sensitive information and should therefore never be written down or stored on-line unless adequately secured. NOTE: Do not use the password storage feature offered on Windows or other operating systems or web browsers unless encrypted with a master password. These features can create a password file that is vulnerable to hackers.
4. Suitable encrypted password stores such as Password Safe are strongly recommended. If you are unsure please contact support@ru.ac.za for advice.
5. Passwords together with user login details should not be inserted into email messages or other forms of electronic communication.
6. Never reveal your password to a Support consultant. You should always type in the password yourself.
7. Passwords that could be used to access sensitive information should be encrypted in transit.
8. The same password should not be used for access needs external to Rhodes (e.g., online banking, benefits, etc.).
9. It is recommended that passwords be changed at least every six months. This may be enforced on some systems.
10. When a forced password change occurs, previous passwords should not be reused. This may be enforced on some systems.
11. Individual passwords should not be shared with anyone, including administrative assistants or IT administrators. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those passwords, and that person will ensure that only appropriately authorized employees have access to the passwords.
12. If a password is suspected to have been compromised, it should be changed immediately.
13. Password cracking or guessing may be performed on a periodic or random basis by systems administration staff in the Information & Technology Services Division or its delegates with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

14. Don’t use your first name, last name, pet’s name, childrens’ names as passwords. All known words including TV show names and dictionary words in any language are hackable.
15. Don’t use all the same letters or numbers in the password.
16. If you have logged in from an open unprotected network somewhere else, you should change your password.
17. Don’t use your login name or the same in any reversible form as a password.
18. As good practice, if you are issued with a password and have not typed in the selected password yourself, you should change the password you are issued with as soon as you receive it.
19. Don’t leave your session logged in. Log out or lock your screen with a password when you leave your station.

Desktop administrator passwords

In addition to the general password guidelines listed above, the following apply to desktop administrator passwords, except where technically and/or administratively infeasible:

20. These passwords should be changed at least every six months.
21. Where technically and administratively feasible, attempts to guess a password should be automatically limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes.
22. Failed attempts should be logged, unless such action results in the display of a failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs for any irregularities or compromises.

Server administrator passwords

In addition to the general password standards listed above, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

23. Passwords for servers must be changed as personnel changes occur.
24. If an account or password is suspected to have been compromised, the incident must be reported to the Lead Systems Administrator via support@ru.ac.za and potentially affected passwords must be changed immediately.
25. Where technically or administratively feasible, attempts to guess a password should be limited to three incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes.
26. It is desirable that the built-in super user (“administrator” or “root”) password for a system be an automatically generated random password. For business continuity reasons, it should be stored in an acceptable enterprise password vault.
27. Uniform responses should be provided for failed attempts, producing simple error messages such as "Access denied". A standard response minimizes clues that could result from hacker attacks.
28. Failed attempts should be logged, unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days.

Administrators should regularly inspect these logs and any irregularities such as suspected attacks should be reported to the Information & Technology Services Division.