General Password Guidelines – Last Amended September 2020

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 contain easily guessed personal information, birthdays, names of family members, pets, etc.
    - not be a your username reversed
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. Never select “remember password”.
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 even where support is required from the I&TS Division. Support staff will require that you are present to log on to any account with your details. You are reminded that an email to support@ru.ac.za creates a ticket in which your password is visible if you have inserted it in the email.
6. I&TS must also ensure that they do not put passwords within RT Tickets.
7. Never reveal your password to a Support consultant. You should always type in the password yourself.
8. Passwords that could be used to access sensitive information should, where possible, be encrypted in transit.
9. The same password must not be used for access to any service external to Rhodes (e.g., online banking, benefits, etc.). When you register for a web site or online app and use your Rhodes email address, never use the same password as your actual email password. Keep your email/internet password unique, generate different passwords for Facebook, Twitter, banking, Takealot etc.
10. It is recommended that passwords be changed at least every six months. This may be enforced on some systems.
11. When a forced password change occurs, previous passwords should not be reused. This may be enforced on some systems.
12. 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 and that the passwords are changed regularly.
13. If a password is suspected to have been compromised, it should be changed immediately. Students who suspect their password for ROSS has been compromised must immediately change their password.
14. Password cracking or guessing applications may be run on a periodic or random basis by the I&TS to ensure that users passwords are compliant and not easy to hack. If a password is cracked or is considered "weak" during one of these scans, the password owner will be required to change it immediately. There will never be a link to the password change site.
15. If you have logged in from an open unprotected network somewhere else, you should change your password.
16. 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.
17. Don't leave your session logged in. Log out or lock your screen with a password when you leave your station.
18. When you leave a public lab, log out of the workstation.

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:

19. These passwords should be changed at least every six months.
20. 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.
21. 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:

22. Passwords for servers must be changed as personnel changes occur.
23. 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.
24. 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.

25. 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.
26. 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.
27. 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.