Stellenbosch University Password Regulations

1. Overview

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 the University's entire network. As such, all University employees (including contractors and vendors with access to the University's systems) and students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The Electronic Communications Policy (ECP) also places the following password responsibilities on the user: to keep passwords confidential and not to share them.

2. Purpose

The purpose of these regulations is to establish **standards** and **guidelines** for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

These regulations are supplementary to the University's Information Security Regulations (I-Sec) and should be read in the context of the latter. It applies to all personnel and students 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 University facility, has access to the University network, or stores any non-public University information.

All passwords must conform to the **standards** below and should preferably follow the **guidelines** also described below. (Refer to the definitions of standards, guidelines and policies in 9).

4. Guidelines and Standards

4.1. System-level and User-level password frequency-of-change standards

4.1.1. All **system-level passwords** (e.g. root, enable, NT admin, application administration accounts, etc.) must be stored separately in sealed envelopes placed in fire-proof safes in the IT computer room and the Disaster Recovery computer room.

4.1.1.1. As a rule these passwords will not be used by system administrators.

4.1.1.2. If the envelope seal is broken, however, the password must be changed, placed back in the envelope and sealed.

4.1.1.3. Should a password be retrieved from the envelope by someone who is not a system administrator, this event is classified as a security incident, the relevant system administrator must be informed, and the password must be changed.

4.1.1.4. Where possible use of such a password should be systemically limited to a network segment or system console.

4.1.2. All **user-level passwords** (e.g. Outlook, Webmail, Novell Netware, WebCT, portal, desktop computer, etc.) must be changed at least every 3 months. Also refer to Single Sign-On (SSO) guidelines in 5.

4.1.3. A special kind of user-level password includes the passwords that system administrators use to administer computer systems. These are not the system-level passwords referred to in 4.1.1. The standard described in 4.1.2 is applicable, except that the SSO password should not be used.

4.2. General Password Construction Guidelines

4.2.1. Passwords are used for various purposes at the University. Some of the more common uses include: Windows accounts, Novell print and file services accounts, portal accounts, WebCT accounts, administrative system accounts, email accounts, screen saver protection, etc. Since very few systems have support for one-time

tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords. Passwords should be easy to remember, but difficult to guess.

4.2.2. **Poor, weak passwords** have the following characteristics:

- 4.2.2.1. The password contains less than eight (8) characters
- 4.2.2.2. The password is a word found in a dictionary
- 4.2.2.3. The password is a common usage word such as:
  - 4.2.2.3.1. Names of family, pets, friends, co-workers, fantasy characters, etc.
  - 4.2.2.3.2. Computer terms and names, commands, sites, companies, hardware, software.
  - 4.2.2.3.3. The words "university", "stellenbosch", "stell", "US" or any derivation.
  - 4.2.2.3.4. Birthdays and other personal information such as addresses and phone numbers.
  - 4.2.2.3.5. Word or number patterns like aaabbb, qwerty, 123qwe, zyxwvuts, 123321, etc.
  - 4.2.2.3.6. Any of the above spelled backwards.
  - 4.2.2.3.7. Any of the above preceded or followed by a digit (e.g. secret1, 1secret)

4.2.3. **Strong passwords** have the following characteristics:

- 4.2.3.1. Contain both upper and lower case characters (e.g., a-z, A-Z)[1]
- 4.2.3.2. Contain digits and punctuation characters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- 4.2.3.3. Can contain spaces, except at the end of passwords
- 4.2.3.4. Are at least eight (8)[2], but not longer than thirty-two (32), alphanumeric characters long.
- 4.2.3.5. Are not words in any language, slang, dialect, jargon, etc.
- 4.2.3.6. Are not based on personal information, names of family, etc.
- 4.2.3.7. Try to create strong 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: "I studied BComm at Maties from 1991 to 1993" and the password could be: "isBC@Mf91~93" or "!sBC@Mf91~93" or some other variation. NOTE: Do not use either of these examples as passwords!

4.3. Password Protection Standards

- 4.3.1. Do not use the password that you use for University accounts for other non-University access (e.g. personal email account, online banking, medical scheme, etc.) as well.
- 4.3.2. Select separate passwords for the administrative systems (the "green screens"), ftp and telnet accounts, and a separate "single sign-on" (SSO) password for other IT systems.
- 4.3.3. Your previous 10 passwords on University systems cannot be re-used.
- 4.3.4. Do not share the University passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive and confidential university information.
- 4.3.5. Here is a list of "don'ts":
  - 4.3.5.1. Don't reveal a password over the telephone to ANYONE
  - 4.3.5.2. Don't reveal a password to the boss

[1] Not all systems distinguish between cases, so it cannot be regarded as a strong security measure.
[2] Ideally, password length should be 8 characters or more, but some systems have limits of 6.

4.3.5.3. Don't talk about a password in front of others
4.3.5.4. Don't hint at the format of a password (e.g., "my family name")
4.3.5.5. Don't reveal a password on questionnaires or security forms
4.3.5.6. Don't share a password with family members
4.3.5.7. Don't reveal a password to co-workers while on vacation

4.3.6. Passwords must not be inserted into email messages or other forms of electronic communication.
4.3.7. If someone demands a password, refer them to this document or have them call the Information Technology (IT) Helpdesk.
4.3.8. Do not use the "Remember Password" feature of applications (e.g. Internet Explorer, Outlook, Netscape Messenger).
4.3.9. Again, do not write passwords down and store them anywhere in your office.
4.3.10. Do not store passwords in a file on ANY computer system (including PocketPCs, smartphones or similar devices) without encryption.
4.3.11. If an account or password is suspected to have been compromised, report the incident to the IT Helpdesk and change all passwords.
4.3.12. Password cracking or guessing may be performed on a periodic or random basis by Information Technology or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

5. Single Sign-on (SSO) guidelines

5.1. Users are encouraged to set all their user-level passwords (Novell network, Outlook/Webmail, Internet/Inetkey) as the *same password*, using the password synchronisation function. This password is also used for portals (mymaties.com, my.sun.ac.za and matiesalumni.net), Sun-e-HR and WebCT access.
5.2. The guiding principle is that if users have to remember fewer passwords, they will select stronger passwords and not store them in obvious places for easy retrieval.
5.3. However, select a *separate password* for the administrative systems (the "green screens").

6. Standards for Retrieving or Resetting Passwords

6.1. Personnel
6.1.1. For the administrative system ("green screens") passwords: contact the system's password administrator and request a password retrieval or change.
6.1.2. For all other passwords personnel must call or email their faculty's computer user area (CUA) manager or the IT Helpdesk. The preferred option is to use the self-service facility; the second option is verifying their identities interactively by means of answers to a number of personal questions; failing that the personnel member must report in person with proof of identity.
6.2. Students must report to their computer user area (CUA) help desk with proof of identity (student card, ID document or passport).
6.3. Distance students (or off-campus personnel members) must use the self-service facility or failing that, call or email their faculty's CUA manager or the IT Helpdesk. Their identities will be verified interactively by means of answers to a number of personal questions. Student numbers and an identity or passport number must be included in the email.
6.4. All requests and changes, including date, time, user whose password was changed, person who facilitated the change and the IP address from which the request was made, will be logged.

7. Application Development Standards

Application developers must ensure that their applications contain the following security precautions:

7.1. should support authentication of individual users, not groups.
7.2. should not store passwords in clear text or in any easily reversible form.
7.3. should never transfer an unencrypted password across a network connection

7.4. should provide for role-based access control, such that one user can take over the functions of another without having to know the other's password.
7.5. should support secure LDAP or RADIUS authentication as relevant, wherever possible.

8. Enforcement

Any user found to have violated these regulations will be subject to consequences as envisaged in the Electronic Communications Policy.

9. Definitions

Terms	Definitions
Guidelines	Typically a collection of system-specific or procedural-specific “suggestions” for best practice. They are not requirements to be met, but are strongly recommended.
Standards	A collection of system-specific or procedural-specific requirements that must be met by everyone.
LDAP	Lightweight Directory Access Protocol
RADIUS	Remote Authentication Dial-In User Service

10. Revision History