**St Joseph's Theological Institute NPC**
(Company number **2003/009125/08**. PBO number **930007111**)
**Registered with the Department of Higher Education and Training as a Private Higher Education Institution under the Higher Education Act, 1997 (Registration Certificate number 2003/HE08/003).**

Private Bag 6004,
Hilton, 3245
Republic of South Africa
website: www.sjti.ac.za
Telephone: +27(87) 353 8940
Facsimile: +27(86) 435 2264
email: president@sjti.ac.za

# PASSWORD POLICY

| | |
|---|---|
| **Title** | Password Policy |
| **Policy No.** | SJTI/ICT/006 |
| **Compiled by** | ICT Consultant |
| **Compiled by** | ICT Consultant |
| **Provisionally Approved by** | President, January 2016 |
| **Reviewed and approved by** | Board of Directors |
| **Review date** | 12 October 2017 |
| **Responsibility for update** | ICT Consultant |
| **Next Review** | October 2020 |

**Purpose of regulation:** To provide a definition of backups to be taken to maintain the integrity of the Institute systems and data

**Regulation applies to:** All Institute staff, students and other authorised users

## 1. Introduction / Rationale

This policy supports the ICT Regulations to ensure that passwords used to access computer resources are selected and updated in line with best proactive security standards.

The Institute ICT Regulations state that Users must take all necessary steps to protect and maintain security of any equipment, software, data, storage area and/or passwords allocated for their use. This policy dictates the minimum that a user must do to conform to this requirement when selecting and updating a password.

Password policies are used to mitigate possible attacks against the Institute's ICT Infrastructure and data held upon it. Use of long, complex passwords helps to mitigate attacks that attempt to guess passwords, and regular password changes to mitigate long term exploitation of any disclosed or discovered passwords.

## 2. Password selection

To protect the Institute's systems and data, users must select a password that is secure and difficult to guess.

In accordance with security best practice the following rules are mandatory:

- All passwords should have a minimum of eight characters,
- Each password must contain a combination of at least three out of four character sets:
  - uppercase characters (A through Z)
  - lowercase characters (a through z)
  - numerical digits (0 through 9)
  - Non-alphabetical characters (e.g.! $ # % @ +)
- Previous passwords used for an Institute system must not be re-used.

In addition, while not actively enforced by the password creation process:

- Accounts created for use on external online resources must not use the same password for Institute authentication.
- Passwords must not be something that can be easily guessed (avoid using your name, children's or a pet's name, car registration number, sports team, etc.)

It is highly recommended that passwords be changed on a regular basis to avoid attempts at identity theft.

**3. Changing a password**

Passwords must be changed at the earliest available opportunity by the user if there is suspicion that the password may be compromised or someone else may know it.
Administrators may also change passwords immediately, or disable accounts if there is suspicion that the passwords have been compromised.

Passwords should be changed regularly to mitigate the long term exploitation of any disclosed or discovered passwords. It is recommended that those passwords are changed every 6-12 months, as is practically convenient.

**4. Password use**

Passwords are the mechanism used to protect the security of Institute systems and must be protected.

- Passwords must be kept secret
- Passwords must not be written in a form that others could identify
- Passwords must not be stored electronically in a non-encrypted format
- Passwords must never be shared with others
- Care should be taken to prevent anyone from watching you type your password