INFORMATION TECHNOLOGY POLICIES

iThemba LABS Amended

Melanie Robertson
melanie@tlabs.ac.za

Table of Contents

Document enquiries can be directed to the IT Department,

Attention: Melanie Robertson

Email: melanie@tlabs.ac.za

Document Review History and Version Control

Version	Date	Change Request	Comment
1.0	2017-11-30	New document	First release

www.tlabs.ac.za

ACCEPTABLE USE POLICY

OVERVIEW

iThemba LABS intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the organisation's established culture of openness, trust and integrity. iThemba LABS is committed to protecting its employees, stakeholders and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

ii. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of iThemba LABS. These systems are to be used for business purposes in serving the interests of the organisation, and of its stakeholders in the course of normal operations.

iii. Effective security is a team effort involving the participation and support of every iThemba LABS employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

PURPOSE

The purpose of the policy is to outline the acceptable use of iThemba LABS IT Services so that users are aware and informed as to what constitutes acceptable behaviour. Unacceptable use of IT Services can place iThemba LABS and others at risk.

SCOPE

iThemba LABS IT Services includes all computer systems (desktops, laptops, servers, storage, network and communication infrastructure) directly or indirectly connected to any iThemba LABS network or telecommunications network. This policy applies to any person(s) using iThemba LABS IT Services.

POLICY

SECURITY

- Ensure that you keep your identity safe and passwords conform to the Password Policy guidelines.
- Ensure that your end-point device operating system and anti-virus are up-to-date when accessing IT Services at iThemba LABS.
- Ensure that the software you install is legally licensed, if not obtain a legal license.
- Ensure you do not infringe on the intellectual property and copyright material of another individual or organisation. E.g. Digitisation and distribution of photographs from magazines, books or other copyright sources, copyright music, and the installation of any copyright software.
- Refrain from using your work email for private use; use a private free service e.g. Google Mail.

NETIQUETTE

Just as certain social norms exist for polite and courteous conduct when interacting with other people face-to-face, so there are similar norms for conduct online.

- Maintaining kindness in all communication in whatever form.
- Sending communication only as yourself.
- Avoiding slanderous, defamatory, offensive, racist, sexist, or obscene remarks.
- Respecting the potential confidentiality of others' communication.

ABUSE OF IT SERVICES

- Excessive Network traffic – should you need to download any large file that might impact IT Services please request permission from the IT Department.
- Misuse of IT services and resources.
- Changes to IT Infrastructure without the knowledge or approval of the IT Department.

UNACCEPTABLE BEHAVIOUR

This policy does not enumerate all possible inappropriate uses but rather presents some guidelines (listed below) that iThemba LABS may at any time use to make a determination that a particular use is inappropriate:

- Downloading of illegal movies, software, music, etc. over the network and storing it on iThemba LABS resources.
- Online gaming during working hours.
- Granting access to an external person or persons to use the iThemba LABS network for the purpose of abusing IT services.
- Excessive use of social networking during working hours - Use of social networks is acceptable within reasonable limits or as defined by the Department Head.
- Using IT Services to run your business from work.

ENFORCEMENT

Violation of this policy may result suspension of access to IT Services or in disciplinary action, in line with the NRF HR Policies.

RELATED DOCUMENTS

NRF Consolidated Information and Communication Technology Policies. URL https://goo.gl/VeI6Y6

iThemba LABS Password Policy.

PASSWORD POLICY

BACKGROUND

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 iThemba LABS's entire network. As such, all iThemba LABS employees (including contractors and vendors with access to iThemba LABS systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

GUIDELINES

Check the TIP Box Below.

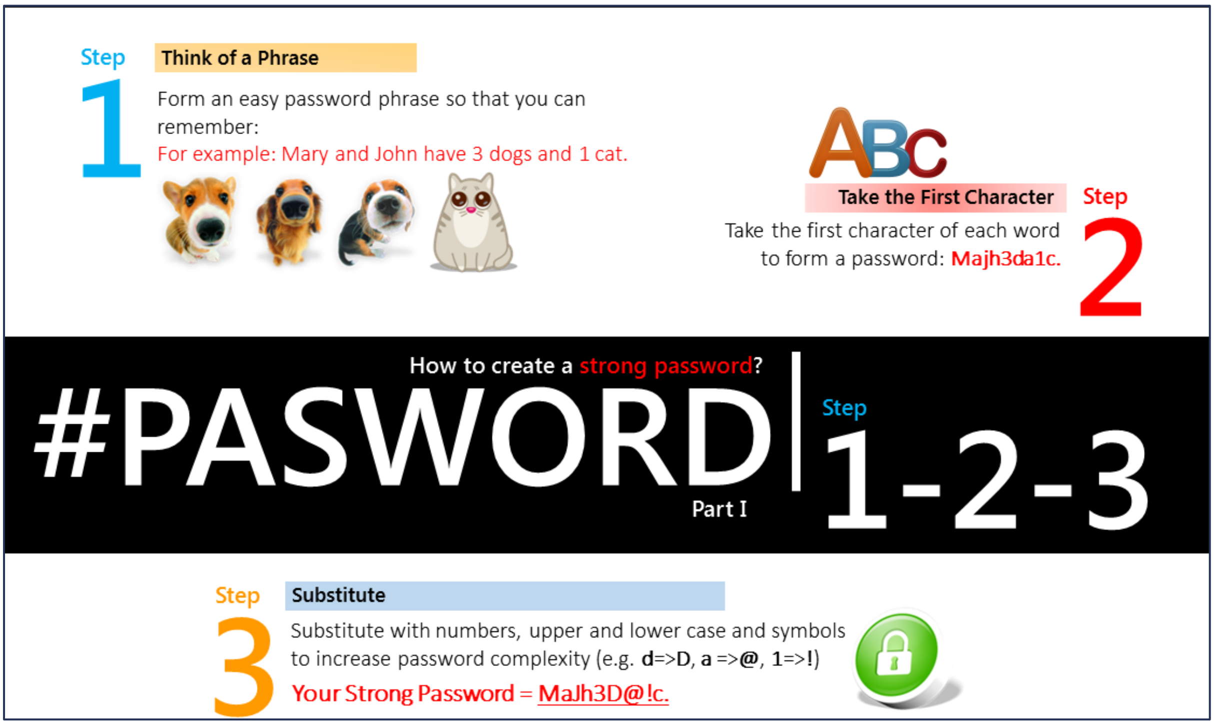
Follow these easy tips to make sure that your password is easy to remember but hard to guess.

- It is at least eight characters long
- Includes at least one character from three of the following categories:
  - Uppercase (A to Z)
  - Lowercase (a to z)
  - Numbers (0 to 9)
  - Symbols (e.g. !,$,#,%. etc.)
- Does not include part of your login or full name

Make Sure ✓

- Write your password down and leave it lying around in full view.
- Use the same password for work and personal activities.
- Re-use your old passwords when asked to change your password.
- Reveal your password for anyone.
- Enable the "Save Password" option if prompted to do so.

Do Not ✗



Step 1 Think of a Phrase

Form an easy password phrase so that you can remember:

For example: Mary and John have 3 dogs and 1 cat.

Step 2 Take the First Character

Take the first character of each word to form a password: Majh3da1c.

How to create a strong password?

#PASWORD Part I | Step 1-2-3

Step 3 Substitute

Substitute with numbers, upper and lower case and symbols to increase password complexity (e.g. **d**=>D, **a** =>**@**, 1=>**!**)

Your Strong Password = MaJh3D@!c.

PASSWORD CHANGING

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on a yearly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every 180 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

REMOTE ACCESS USERS

Access to the iThemba Networks via remote access is to be controlled by the network / domain administrators. Access is granted via a formal request and activated accordingly.

ENFORCEMENT

Violation of this policy may result in disciplinary action, in line with the NRF HR Policies.

RELATED DOCUMENTS

NRF Consolidated Information and Communication Technology Policies. URL https://goo.gl/VeI6Y6

LOGICAL ACCESS POLICY

OVERVIEW

iThemba LABS provides user/network accounts for accessing the computing facilities and associated resources to authorised users. In order to facilitate the effective operation of the institution, it is expected that users will conform with all the rules and regulations pertaining to the appropriate use of these facilities.

Logical access control measures are put in place in order to prevent the possible compromise of information, IT assets and facilities under the control of iThemba LABS, as a means to protect information and its communications infrastructure in general. Every user is responsible for helping to ensure that these resources are used appropriately. If someone is in doubt as to whether a particular proposed use is appropriate, they should check with the Information Technology (IT) department before the proposed use is undertaken.

PURPOSE

This process establishes a standard for the account administration of computing accounts for authorised users of the lab. This policy is an adjunct to the labs Acceptable Use Policy which defines the acceptable behaviour expected of users and intending users of the institution.

SCOPE

This policy applies to all user accounts (or any form of access that supports or requires a User/Network ID on any system at iThemba LABS, has access to the iThemba LABS network, or stores any non-public iThemba LABS information.

POLICY

1. Process for obtaining an account

Accounts are created for various individuals depending on their role and purpose.

A user’s manager, or, in the case of a new employee, HR, must submit a request for the creation of a new account to the IT Service desk by completing an Account Request form. If submitted via HR the account will only be activated once the user has presented him/herself to the IT department and signed the requisite forms.
A new user is not permitted, under any circumstances, to inherit the User/Network ID that was originally assigned to another user. Before access is given to an account, all users should be informed about NRF and iThemba LABS IT Policies.

2. General Requirements

- All accounts must be uniquely identified using the assigned username.
- Passwords should be in-line with iThemba LABS Password Policy.
- Any accounts not accessed within 90 days of creation will be disabled.
- Modification requests of account name changes, permission changes or change of user role requires the signature of the requestor’s supervisor / manager / HR.

- Application Access accounts are requested via the System Administrator of the relevant system e.g., Gate system.
- There are some systems at iThemba LABS that require more than one user id and password for access to data.
- All e-mail accounts are created with an e-mail quota, an increase to the e-mail quota of an account may be permitted if approved by the System Administrator.
- Temporary passwords for new accounts will be emailed to remote users. Users will be required to change it at first logon.
- The date when the account was created will be recorded in an audit log.
- When establishing accounts, standard security principles of "least required access" to perform a function will be used, where administratively feasible.
- Accounts on all systems need to be audited annually for validity.

3. User Account Termination

Staff

- Once termination notification has been received from HR and if it is voluntary termination, accounts are disabled and access removed the last working day by the IT Service desk. The account will live on the system for 180 days before deletion.
- Accounts will only remain active if requested by the relevant manager as the account holder will continue to have a relationship with the facility, but the user will have limited access.
- If involuntary termination, accounts are disabled and access revoked immediately.

Students

- Accounts are disabled and access removed on the termination date as listed in the Account Request form.
- Accounts will only remain active if the relevant supervisor/ manager has indicated that the student term has been extended through filling a request.

External Users

- Student termination process will apply.
- All external users must belong to a department where the relevant manager / supervisor must file a request should the visit be extended.

System Accounts

- Upon termination of a System Administrator, on the last day the account is disabled, all access removed and system passwords changed.

Email Accounts

- Termination process will be determined by the type of account holder, (eg., staff, student)
- E-mail will be archived, this will be dependent on iThemba LABS storage space. Preference given to staff account holders.

- Email accounts are accessible for 30 days after termination and thereafter disabled. The email system administrator, upon request will forward e-mail to the new e-mail address for 60 days once formal approval has been granted.

4. Contact Directory

The name and contact details of an individual is accessible through the iThemba LABS telephone book application located under \\oberon\users_common\TLabs Phone Book
Or with Active Directory Search.

5. Monitoring of User /Administrator Accounts

Accounts will be monitored and verified at least annually and signed off.

ENFORCEMENT

Violation of this policy may result in disciplinary action, in line with the NRF HR Policies.

RELATED DOCUMENTS

NRF Consolidated Information and Communication Technology Policies. URL

https://goo.gl/VeI6Y6 .

iThemba LABS Password Policy.

NRF National Research Foundation | iThemba LABS Laboratory for Accelerator Based Sciences

www.tlabs.ac.za

USER ACCOUNT MANAGEMENT POLICY

OVERVIEW

User account management is an integral part in protecting potentially sensitive organisational network and information resources from unauthorised use. Account administration and monitoring provides a mechanism to protect information and information systems through the proper construction of secure user accounts and the proper management of them.

PURPOSE

This process establishes a standard for the account administration of computing accounts that facilitate access or changes to the iThemba LABS network or applications. Through this process, standards for issuing and managing accounts are established.

SCOPE

This process is applicable to those responsible for the management of the IT network, user and system application accounts. This process covers access to network and application accounts and should be used in line with the iThemba LABS Logical Access Policy.

POLICY

The purpose of this policy is to establish the requirements for managing access on all accounts for any IT systems or applications supported by iThemba LABS.

Authority, Responsibility and Duties

Roles and responsibilities are assigned to individuals and may differ from their positions.

System Owner

Is responsible for the following relative to the system he/she owns:

1. To establish the roles and access levels for the system.
2. Approving all access request to their system.
3. Reviewing on a periodic basis (at least annually) all user accounts for the system for validity.
4. Determining the cause of unusual IT system access activities. With the System Administrator, to investigate any unusual IT system access activities and approve changes to access level authorizations.

System Administrator / System Support

Is responsible for the following relative to the systems he/she administers:

1. Co-operating with authorized management investigating incidents where possible breaches of IT Policies occur.
2. Using administrative accounts only when performing administrative task.
3. Staff can be granted privileged accounts that permit elevated access rights for specific system or application support and maintenance.

4. Generic/built-in privileged accounts (e.g., Windows domain and local administrator, etc.) shall not be used for daily systems administration.

Service desk

Is responsible for the following:

1. Setting up only authorized accounts as per the User Account Request form.
2. Disabling accounts of terminated employees.
3. Modifying user accounts to accommodate situations such as name changes, access privileges or users that change roles within the institution with proper authorization.
4. Reviewing existing accounts periodically for validity (at least annually) and obtaining departmental approval/sign-off.
5. Conducting independent audit review of accounts and access administered
    - Providing a list of accounts and access privileges he/she administers when requested by authorized management
    - Co-operating with authorized management investigating incidents where possible breaches of IT Policies occur.

Human Resources

The Human Resources department is responsible for

1. Providing timely information regarding new employees and termination or modification of employment status to the IT Service desk.
2. Providing a list of terminated employees for the purpose of auditing system accounts upon request.

All users of Electronic Resources and Systems are accountable for any activity on the system performed with the use of their account.

ENFORCEMENT

This policy defines the responsibilities and management of user account at iThemba LABS, non-adherence to this procedure may result in disciplinary action in line with NRF HR Policies.

RELATED DOCUMENTS

NRF Consolidated Information and Communication Technology Policies. URL https://goo.gl/VeI6Y6

iThemba LABS Logical Access Policy