WSU

Walter Sisulu University

WALTER SISULU UNIVERSITY COMPUTING PASSWORDS POLICY

Policy library ID
ICT: 02

WSU
Walter Sisulu University

Computing Passwords Policy

Sponsor division	Operations and ICT Services
Responsible Department	ICT Services

Related WSU policies

Policy name	**Policy Name**
Acceptable Use Policy	IT Security Policy

Change History

Approval authority	**Council**
Approval Date	**01 July 2016**
Latest revision date	**01 July 2016**
Effective date	**Immediately**

Chairperson of Council

Contents

1. PREAMBLE

1.1 Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data.

1.2 The drafting and the use of all ICT Passwords must therefore adhere to this policy.

2. PURPOSE

This policy describes the Walter Sisulu University (WSU) requirements for acceptable password selection and maintenance to maximize security of the password and minimize its misuse or theft.

3. SCOPE

This policy is relevant to anyone accessing or utilizing WSU's network resources or data facilities. This use may include, but is not limited to, the following: personal computers, laptops, cell phones, desktop telephones (PINS) and hand-held computing devices such as tablets, USB flash disks and external drives. The policy also covers WSU information technology services, systems and servers.

4. DEFINITIONS

Any definitions listed below apply to this document only with no implied or intended institution-wide use.

"Administrator" – someone whose job is to control the operation of a resource in an organization.

"Data Trustees" – entities accountable for the security, privacy, data definitions, data quality and compliance to data management policies and standards for a specific domain.

"Identity Theft" - obtaining the personal information of another person for the sole purpose of assuming that person's identity in order to make transactions.

"Multi-factor Authentication" – a method of computer access control in which a user is only granted access after successfully presenting several pieces of evidence, typically two of the following categories; knowledge (something they know) and possession (something they have).

"Password" - a sequence of characters that allows access to a computer, an interface, or a system.

"Shared Data" – data stored in one or more servers in the network with some software locking mechanism that prevents the same set of data from being changed by two entities at the same time.

5. POLICY IMPLEMENTATION

5.1 General Passwords guideline

5.1.1 All passwords should be strong and follow the standards listed below. In general, a password's strength will increase with length, complexity and frequency of changes.

5.1.2 Greater risks require a heightened level of protection. Stronger passwords augmented with alternate security measures such as multi-factor authentication, should be used in such situations. High risk systems include but are not limited to: systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

5.1.3 Central and departmental account managers, data trustees, and security and/or system administrators are expected to set a good example through a consistent practice of sound security procedures.

5.1.4 All passwords should meet the following minimum standards, except where technically infeasible:

a. Be at least eight alphanumeric characters long
b. Contain digits or punctuation characters as well as letters (e.g., 0-9, + ? . * ^ \$ ( ) [ ] { } / ~ ! \ @ # & = , -)
c. Contain both upper and lower case characters (e.g., a-z, A-Z)
d. Not be a word in any dictionary, language, slang, dialect or jargon
e. Not be solely based on easily guessed personal information, birthdays, names of family members and pets

5.1.5 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.

5.1.6 All passwords are to be treated as sensitive information and should therefore never be written down or stored online unless adequately secured.

5.1.7 Passwords together with user login details should not be inserted into email messages or other forms of electronic communication.

5.1.8 Passwords that could be used to access sensitive information should be encrypted in transit.

5.1.9 The same password should not be used for access needs external to WSU (e.g., online banking).

5.1.10 It is recommended that passwords be changed regularly. This may be enforced on some systems.

5.1.11 When a forced password change occurs, previous passwords should not be reused. This may be enforced on some systems.

5.1.12 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.

5.1.13 If a password is suspected to have been compromised, it should be changed immediately.

5.1.14 Password cracking or guessing may be performed on a periodic or random basis by systems administration staff in the Information & Technology (ICT) Services Department. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

5.1.15 Do not use the "remember password" feature which some websites offer to keep you logged in whenever you click a check box on the site.

5.2 System 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:

a. These passwords should be changed at least every three (3) months.
b. Attempts to guess a password will be automatically limited to three incorrect guesses. Access will then be locked for a period of 30 minutes.

c. 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 90 days. Administrators should regularly inspect these logs for any irregularities or compromises.

5.3 Server Administrator Passwords

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

a. Passwords for servers must be changed as and when personnel changes occur.
b. If an account or password is suspected to have been compromised, the incident must be reported to the responsible manager and potentially affected passwords must be changed immediately.
c. Attempts to guess a password will be limited to three incorrect guesses. Access will then be locked for a period of 30 minutes.
d. The strength of server administrator passwords will be tested. Only passwords that pass the test will be adopted.
e. 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.

5.3.2 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 90 days. Administrators should regularly (weekly) inspect these logs and any irregularities such as suspected attacks should be reported to the responsible manager.

5.4 Passwords on Specific Servers

5.4.1 For specific systems, additional or different requirements may be enforced by the administrators of those systems. However, such requirements must continue to meet the spirit of this policy.

5.4.2 Log files should never contain password information.

6. POLICY REVIEW

This policy should be reviewed every three years, or as changes in legislation or technology dictate.

7. RELATED POLICIES

a. Acceptable Use Policy
b. IT Security Policy