Document Name	Policy on Passwords
Language(s)	English
Responsible Unit	UGC Standing Committee on Computing
Creator (individual)	UGC Standing Committee on Computing
Subject (taxonomy)	Password Management
Date created	22 March 2012
Date to be adopted	31 December 2012
Mandatory Review	January 2014
Audience	These policies and procedures are to be used by all Staff Members of University Staff, Associates, Students, Public resisted users who access computing resources which are controlled by access control technologies. System developers, System Architects, system administrators & Help desk technical Staff.
Replaces	None
Is part of	Computing Policies and Standards
Related documents	Policy on Use of Computing Resources

Version	Date	Author(s)	Revision Notes
1	22 March 2012	UCSC – Mr. C.M.B. Attanayake & Prof. G.N. Wikramanayake	First version V0.10
2			

TABLE OF CONTENTS

SECTION 1. INTRODUCTION

The University promotes the use of computers to share information and knowledge in support of academic administrative and management activities. Majority of computer systems utilized password, Passphrase or PIN (Personal Identification Numbers). This document establishes the framework for such authentication policy and standards for University computing resources and data and is to be applied within the relevant context of:

- University Policy on use of Computing Resources.

SECTION 2. GENERAL PROVISIONS

2.1 Reason for Issue

The main purpose of this document is to establish policy on password creation, usage and protection to ensure confidentiality, integrity, availability, and privacy in computing resources and data and to inform University users about the applicability of this policy when utilizing University computing resources and data.

2.2 Scope

This policy shall apply to:

a. All University Staff Members and Associates.

b. All university students

c. All Technical support staff

d. All technical staff involve in development, designing, implementing and managing computer systems

SECTION 3. PASSWORD\ PASSPHRASES IMPLEMENTATION

3.1 Password Classification

Due to various systems and technologies passwords are classified on the following manner.

Password Class	Minimum Length	Complexity	Maximum Password Age (lifetime)
Class A	16	Alpha numeric+ symbols	30 days
Class B	12	Alpha numeric	45 days
Class C	8	Alpha numeric+ symbols	90 days
Class D	8	Numbers only	30 days
Class E	8	Numbers only	90 days
Class F	4	Numbers only	30 days
Class G	4	Numbers only	90 days

3.2 Password Complexity

a. All system and privilege passwords of systems must be Class A passwords.

b. All user accounts Passwords of systems containing Sensitive information must be Class B passwords.

c. User passwords for generic systems (e-mail, Intranet, etc.) must be class C passwords.

d. Users shall uses class D,E,F,G Passwords only in the case of absolute technical impossibility to use alphanumeric characters such as Phone system, Photocopy, access doors.

e. All remote access technologies used on telephony systems (PABX) such as DISA (direct System inward Access must use Class D passwords, or combination of PIN and password to access international lines.

f. All telephony systems with international dialing facility shall satisfy class E password implementations.

g. Service or privilege accounts of none critical computing resources such as access doors, photocopy, etc. shall uses Class F passwords.

h. All users accounts on none critical computing resources such as access doors, photocopy, etc. shall uses Class G passwords.

i. Password should not contain the user’s system name or any part of the user’s real name.

j. Users must choose difficult-to-guess passwords. This means that passwords must not be in the dictionary and must not be a reflection of the user’s personal life. For example, license plate number and spouse’s name are both unacceptable passwords.

k. User accounts that have system-level privileges granted through group memberships or programs such as “Admin”, “Administrator”, “root”, "sudo" must have a unique password from all other accounts held by that user.

3.3 Changing Passwords

a. Users must provide their old password to be allowed to choose a new password.

b. Passwords may not be reset to any of the user’s three previous passwords.

c. Switching between two or a similar small number of passwords is therefore prohibited.

d. Where possible, users should be given a warning that their passwords are going to expire at least five days but not more than ten days prior to expiration.

e. Where systems support it, expired passwords feature must not be employed.

f. If Users suspect that somebody else may know their password, the password must be immediately changed and report the incident to the Head of the department and the head of Computer unit.

g. The Help Desk will not reset user passwords unless a user first definitively identifies him- or herself.

3.4 Initial Setup

a. The initial password must meet the complexity requirements outlined above.

b. Users must be required to change the password the first time it is used.

c. All passwords set by default by the hardware or software vendor must be changed upon installation.

3.5 Password Storage

a. Users must not store their passwords in any computer (including Palm Pilots or similar devices) or computer files (such as log-in scripts or computer programs) unless the passwords have been encrypted with proper encryption software.

b. Such passwords must be stored using a non-reversible encryption algorithm.

3.6 Password Transmission

a. Passwords should not be sent in unencrypted e-mail messages.

b. When encryption is not practical, a password and the user's system name that it corresponds to must not be transmitted in the same e-mail message.

c. System administrators shall use alternative password transmission technique (sms, phone, verbal) when transferring initial password and must not uses unencrypted email, fax or any unsecured transferring techniques.

3.7 Account Lock-outs

a. User accounts must be locked out after no more than three successive invalid access attempts in no less than fifteen minutes.

b. A locked account must remain locked for at least fifteen minutes or until a security management administrator manually unlocks the account.

3.8 Generic Account/ Service Accounts

a. One individual must be accountable for each user account.

b. Access must not be provided through shared "guest" accounts.

c. Accounts set up for training purposes must be assigned to no more than one person at the same time. Passwords must be changed when accounts are reassigned.

d. Users who require privileged access should be given their own privileged account, rather than share a generic account.

3.9 Administrator Accounts and Other Privileged Access

a. Names of "administrator" accounts should be changed from their default values, where possible.

b. All production system-level passwords must be part of Computing Security administered global password management database.

c. Password aging and complexity requirements must be followed.

d. A printed copy of system and Privileged account passwords shall be kept in sealed sign envelope in the custody of the head of the Computer unit for emergency purpose.

e. Administrator or Privileged account passwords must not be given to venders or outsiders for any reason. The passwords must be reset before handing over a computer resource to vender for maintenance or repair work and it must be reset again when the vender return it back to university.

3.10 Passwords Protection

a. Users must not share a password with anyone, including members of their family, their manager or co-workers. Instead, Users must employ authorized mechanisms to share information such as local server shared directories, electronic mail, intranet pages, or floppy disks. Co-workers who need to back-stop users during an absence should arrange for temporary access in their own names. Please see Section 5.3 of the Policy on Use of Computing Resources on the topic of password protection and accountability.

b. Passwords must not be written down unless they have been concealed by a transformation process, or they are physically secured (such as placed in a locked file cabinet).

c. Users must not use the same password for accessing computing resources provide by University and for other non-University access (e.g., personal ISP account, Gmail).

SECTION 4. PASSWORD/PASSPHRASES USAGE GUIDELINES

4.1 Selecting proper passwords

a. Always use strong passwords which:

   i. Are at least eight characters long.

   ii. Does not contain your user name, real name, or company name.

   iii. Does not contain a complete dictionary word.

   iv. Are significantly different from previous passwords.

   v. Contain characters from at least three of the following four groups:

      1. Uppercase letters (A, B, C, … Z)
      2. Lowercase letters (a, b, c, … z)
      3. Numerals (0, 1, 2, … 9)
      4. Non-alphanumeric symbols

b. Strong passwords are easier to remember when memory techniques are employed; for example, several familiar words can be strung together or an acronym can be derived from words in a favorite song.

4.2 Security of the password

a. Never reveal your passwords in person, over the phone, or electronically.

b. Don’t talk about your passwords in front of others, even in general terms.

c. Help desk and system administration staff should never need to ask for a password. If someone contacts you and tries to convince you to reveal a password, report the incident to the head of the computer unit.

d. Security forms do not require you to provide a password. Be suspicious of any form that requires you to reveal a password.

e. Be careful about where passwords are saved on computers. Some dialog boxes present an option to save or remember a password. Selecting this option poses a potential security threat and must not select the option on public or shared computers or devices.

SECTION 5. DEVELOPER GUIDLINE

5.1 Application Development Standards

a. Application developers must ensure their programs are complying with the policy.

b. Applications should support authentication of individual users, not groups.

c. Applications should not store passwords in clear text or in any easily reversible form.

d. Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Applications should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

5.2 Use of Passwords and Passphrases for Remote Access Users

a. Access to the University Network via remote access shall controlled using either a one-time password authentication or a public/private key system with a strong passphrase. The remote access is preferred to be provided through VPN technologies

SECTION 6. FINAL PROVISIONS

6.1 Violations of Policy

a. As this policy is integral to the Policy on Use of Computing Resources, Section 7.2 of the Policy addresses this topic.

6.2 Effective Date

This policy shall enter into force on or before 31st December 2012.

SECTION 7. DEFINITIONS

Alphanumeric Is a combination of alphabetic and numeric characters or a text constructed from this collection.

Associates Any visitor who is on official agreement with the Institution.

Authorized User Any staff member (see definition below), student or resisted public users who are authorized to use computing resources.

DISA Directs Inward System Access. A technology used by telephony systems to allow users to gain access to the system from remotely.

Encryption Is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable

LDAP Lightweight Directory Access Protocol is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

PABX Private Automated Branch Exchange is the private telephone network used within the university

PIN Personal Identification Number A number given from a system to identify a person.

Privilege accounts Account which has special functional ability than normal users. E.g. :- admin, su

RADIUS Remote Authentication Dial In User Service is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

Staff Member An institution employee as defined by a written contact.

TACACS+ Terminal Access Controller Access-Control System Plus is an access control network protocol for routers, network access servers and other networked computing devices.

VPN Virtual Private Network is a network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or traveling users an access to the central organizational network.

X.509 ITU-T standard for a public key infrastructure (PKI) which define standard for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.