The University of Macau
Guidelines for User Account and Password

Document code:	ICTO.11/201806/008.r00
Approval date:	28 June 2018
Effective date:	28 June 2018
Supersedes:	Nil

Keywords*: account, password, user account*

Remarks:

1. INTRODUCTION

These guidelines are established to provide guidance for all students, staff and users of the University of Macau (UM) on the usage of user account and password as well as to provide recommendations on how to securely maintain and manage user account and password.

2. SCOPE

These guidelines apply to all students, staff and users who have a set of user account and password on at least one UM system or application, regardless of whether he or she is an end user, a supporting staff or a system administrator for that system or application.

3. DEFINITIONS AND CONVENTIONS

3.1. Definitions

User ID	User ID is used for identifying a user in a computer system or application.
Password	Password is used for user authentication and identity proof.
User Account	User account consists of user ID and password. The password associated with a user ID is used for verifying one's identity which he or she claims to be.
Individual	Any student, staff or user who has a set of user account and password on at least one UM system or application, regardless of whether he or she is an end user, a supporting staff or a system administrator for that system

	or application.
Privileged user	Individual who has higher authority and access to a system than general individual, such as root access, help desk support, system administrator, etc.
Privileged account	User account of privileged user.
Least Privilege	The principle of least privilege requires that an individual should be given no more privilege than necessary to perform a job.
Strong Password	A password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.
ICTO	Information and Communication Technology Office
DICTO	Director of ICTO
IST	Information Security Team of ICTO

3.2. Conventions

The following is a list of conventions used in this document:

Shall	The use of word "shall" indicates a mandatory requirement.
Should	The use of word "should" indicates a best practice, which should be implemented whenever possible.
May	The use of word "may" indicates a desirable best practice.

4. INDIVIDUAL RESPONSIBILITIES

These guidelines shall observe the ICTO.04/201210/001 - "Acceptable Use Policy on ICTO Computing Facilities, Campus Network and Internet".

Individuals are responsible for keeping passwords secure and confidential. As such, in order to create and safeguard the passwords, the following principles shall be adhered to:

4.1 Passwords shall be changed immediately upon issuance for the first-use including new account creation and reset password, etc.

4.2 Passwords should be strong enough (Refer to 6.2).

4.3 Password should be changed periodically.

4.4 Passwords shall **not** be written down and left in a location easily accessible or visible to others.

4.5 Passwords shall **not** be stored in a web browser's password manager on an untrusted device.

4.6 Passwords shall be securely delivered to corresponding user if the individual need to handle or manage other user accounts.

4.7 Individuals shall use different passwords for different accounts.

4.8 Individuals shall be responsible for all activities performed with their user IDs. They shall use their user IDs to perform authorized tasks and functions only.

4.9 User accounts shall **not** be associated with any app or website which is not approved officially.

4.10 Passwords shall be changed immediately if individual suspects that it has been compromised.

4.11 Individuals shall **not** share password with anyone for any reason including technicians, helpers, supervisors and system administrators, etc.

4.11.1 Unless it is unavoidable due to needs.

4.11.2 Any exemption, which is not listed as common situation with pre-approval in the Appendix I, shall obtain explicit approval from DICTO with supporting reason. The form – "Application for Shared User ID and Password" shall be filled with the corresponding justification. IST shall justify the usage against the security risks that a system may expose to. IST shall review the need periodically and remove the shared account when the justifications are no longer valid.

5. PRIVILEDGED USERS RESPONSIBILITIES

Privileged users shall also observe the guideline stated in "4. INDIVIDUAL RESPONSIBILITIES". If there is any contradiction between Section 4 and this section, this section shall take precedence.

5.1. Controlling the Use of Special Privileges

For the rights of privileged user, the following shall be considered to restrict and control the use:

5.1.1. Special privileges associated with each system or application, and the individuals whom they need to be allocated, shall be identified.

5.1.2. Special privileges shall be granted to individuals based on the principle of least privilege and segregation of duties.

5.1.3. Special privileges should be granted to a user ID different from those used for regular activities.

5.1.4. Regular activities should not be performed by privileged user IDs.

5.1.5. Specific procedures should be established to avoid the unauthorized use of default administration user IDs.

5.1.6. The list of privileged user accounts should be reviewed at least annually to ensure appropriate access and documentation of the review should be maintained.

5.2. User Account Handling

5.2.1. Individual accountability should be established so the respective individual be responsible for his or her actions in systems.

5.2.2. User accounts shall only be issued to those who are eligible for an account and whose identity has been verified. When the account is created, a unique User ID will be assigned to the individual for his or her own use. User IDs shall not be recycled;

5.3. Password Handling

5.3.1. Shall change all system or any default passwords, including service accounts after installation of a new system.

5.3.2. Shall define a strict password policy. (Refer to Appendix II)

5.3.3. Shall not reset an individual's password unless his or her identity can be verified.

5.3.4. Shall not ask for an individual's password.

5.3.5. Shall not allow the password file/database to be publicly readable.

5.3.6. Shall use different passwords as initial passwords for different accounts.

5.3.7. Shall technically enforce or request the individual to change the initial password immediately upon receiving the new password.

5.3.8. Shall technically enforce or request individuals to change their passwords periodically.

5.3.9. Shall securely delivered passwords to corresponding individual.

5.3.10. Shall scramble passwords with one-way functions.

5.3.11. Shall deactivate a user account if the logon fails for multiple consecutive times.

5.3.12. Shall remind the responsibilities of the individuals in protecting their passwords.

5.4. User Privileges Handling

User privileges shall be reviewed periodically and the following shall be considered and put into action:

5.4.1. Authorization for access should be governed by the owner of the system. Level of access granted shall be verified and appropriate based on business purposes and other security controls;

5.4.2. Privileged access rights should be checked to ensure no unauthorized access.

5.4.3. Access rights for individuals who change roles or positions within the organization shall be revised as appropriate.

5.4.4. User privileges, including temporary and emergency access, shall be revoked after a pre-defined period of inactivity.

5.4.5. User privileges shall be revoked when they are no longer required, e.g. upon a staff's termination of employment or change of position.

5.4.6. If a departing staff has known passwords for user IDs which will remain active, these passwords should be changed upon termination or change of position.

6. REFERENCE

6.1. ICTO.04/201210/001 - "Acceptable Use Policy on ICTO Computing Facilities, Campus Network and Internet"

6.2. FAQ - "How to choose a strong password"

If you have any questions, please contact the ICTO Helpdesk.

Appendix I Pre-approved situation for sharing user ID and password

In case of sharing user ID or password is unavoidable, it shall obtain explicit approval from DICTO with supporting reason. In order to simplify the approval procedure, the pre-approved situations with specific conditions* are listed as below.

- Appliance with ***single*** administration account or password including computer BIOS/CMOS password and remote management password. It shall be connected to a restricted management network.
- System service account with least privilege, log in restriction and unauthorized login detection.
- Kiosk type computer for public use or specified group of persons. The account shall be granted with least privilege, log in restriction and unauthorized login detection.
- Password-protect program setting on End-point security tools and the password shall be managed by the central management console.
- Windows 7 XP-mode password which cannot be used for remote login.
- Appliance root account for mass deployment such as network switches whose remote access is restricted to limited management network.

Appendix II Password Policy

A password is served as a security measure against unauthorized access to system and data. The password policy shall be carefully defined and documented for each category of accounts balancing the security requirements and operational efficiency. The password policy shall at least include the following as far as practical.

- Minimum password length
- Password complexity
- Password life cycle (history)
- Account lockout
- Regular password change