CITY UNIVERSITY OF HONG KONG
Password Management and Multi-Factor Authentication Policy for User and System Accounts

---

(Approved by the Information Strategy and Governance Committee in August 2023)

Document Control

Document Owner	Classification	Publication Date
CSC	INTERNAL	2023-08-31

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2023-01-28	Revised the link and reference material in this document. Added Multi-factor authentication (MFA) objective in section 1. Updated Password Strength requirements in section 4. Added section 5. Multi-Factor Authentication Requirements
1.2	2023-08-31	Removed “Minimum password age” in section 4.

Distribution

Copy	Issued to	Location
Master	All University Units	CSC Website

Contents

1 Objective

The objective of this policy is to establish a standard for the creation of passwords with sufficient strength, the protection of those passwords, and the frequency of change. In addition to password management requirements, use of multi-factors authentication to uplift overall security level is required.

Weak and/or long-life passwords are often used by attackers and automated password crackers to gain unauthorized access to information systems. To defend against misuse or theft, password must therefore adhere to this policy.

In the older days, traditional password-based authentication relies only on a user's login credentials (username and password) to check access attempt to an enterprise system. This "single-factor" authentication method is considered as not secure or reliable enough.

Multi-Factor Authentication (MFA) does not rely only on the user's credentials for authentication. Instead, it asks the user to provide more than a single authentication factor to verify their identity. The secondary authentication factor can be one-time password, push verification from mobile app or hardware security token. Only when the system can verify all the factors, will it allow a user to access the system. Thus, MFA helps ensure that a user really is who they say they are. It also provides stronger and more reliable security against cyber threats compared to password-only systems.

2 Scope

This policy applies to all users, and system accounts of the University either hosted internal or external/cloud. This policy covers both central and departmental systems.

All system owners or controllers, including central and departmental systems, are responsible for ensuring that access control in their systems are managed in a manner that is compliant with this policy.

3 Password Protection Requirements

User accounts (U) are used by systems to authenticate individual users, and system accounts (S) are used by administrators to maintain the system. The account holders must protect their passwords as follows:

3.1 (U,S) All passwords must meet the "password strength requirements" defined in the next section, unless technically infeasible to do so. In case any of the requirements could not be complied, the exemption must be documented, compensated by additional security controls, and endorsed by appropriate authority, e.g. Head of Department of system owner or controller.

3.2 (U,S) All passwords must be treated as "Confidential" information and should not be written down or stored on-line unless adequately secured.

3.3 (U) Individual passwords must not be shared with anyone, including supervisors, peers and subordinates.

3.4 (U) Use different passwords for different University Central IT services, i.e. “Active Directory (AD)” earlier known as “Network Connection Password”, “LDAP” earlier known as “Application Password”, and cloud services provided/subscribed by the University.

3.5 (U,S) The same password should not be used for both University Central IT services and external services (e.g. personal online banking).

3.6 (U) Individuals who forgot their passwords must follow CSC procedures strictly in resetting corresponding passwords.

3.7 (U) On resetting passwords which overrides all passwords in University Central IT services to the same new password, the individual must further change the password of either AD, LDAP, and/or cloud systems, so that they will all have different new passwords (compliance to Point 3.4 and 3.5).

3.8 (S) If necessary, sharing of system accounts must be limited to trained administrators on a need-to-know and need-to-use basis. System owners must maintain records of password holders and change password immediately when there is personnel change.

3.9 (U,S) Do not use the “Remember Password” feature of applications (e.g. Internet Explorer). If unavoidable, e.g. mobile devices, apps, screen saver with adequate password strength must be used.

3.10 (U, S) Account name and password must be distributed separately and without reference to each other.

3.11 (U, S) Passwords must be encrypted for storage and in transit.

3.12 (U, S) If an account or password is suspected to have been compromised, report the incident to CSC, and change all related passwords immediately.

3.13 (U, S) Password cracking or guessing may be performed in a period or random basis by authorized security professionals. If a password is revealed or suspected to be revealed, the user will be required to change it immediately.

4 Password Strength Requirements

The following minimum password strength requirements will be enforced on all user accounts managed by Central IT. Departments are required to enforce same policies on departmental systems. Stronger password should be used for accounts or systems holding more valuable data.

Requirement	**Baseline Setting**	**Description**
Password history	3	the number of unique new passwords that must be associated with a user account before an old password can be reused
Maximum password age	365 days	the period of time (in days) that a password can be used before the system requires the user to change it
Minimum password length	8	the least number of characters that can make up a password
Maximum password	64	the biggest number of characters that can make up a password
Password must meet complexity requirements	Enabled	The password contains characters from ALL of the following categories: • Uppercase letters of European languages (A through Z) • Lowercase letters of European languages (a through z) • Base 10 digits (0 through 9)
Account lock-out threshold	10	the number of failed logon attempts that will cause a user account to be locked-out
Account lock-out duration	30 minutes	the number of minutes that a locked-out account remains locked-out before automatically becoming unlocked
Reset account lockout counter after	15 minutes	number of minutes that must elapse from the time a user fails to log on before the failed logon attempt counter is reset to 0
Force users to change their passwords at the first log-on.	Yes	The system should force user to change their password at the first log on or after password reset

5 Multi-Factor Authentication Requirements

The following minimum multi-factor authentication (MFA) requirements will be enforced on all user accounts managed by Central IT. Departments are required to enforce same policies on departmental systems.

5.1 All staff and student shall activate MFA to safeguard University resources and data.

5.2 MFA shall be used for accessing an information system that stores information classified as CONFIDENTIAL or above.

5.3 MFA shall be used for accessing an information system as required by Central IT or respective system owner.

5.4 University user shall be challenged with MFA sign in for new devices for the first time.

a) Sign in from a browser without an HTTP cookie (e.g. Microsoft Edge in-private mode, Chrome incognito mode)

b) Sign in from a browser which has just cleared all cookies

c) Sign in from a computer with “reborn” (restored automatically to its original setup on every system restart) setup.

d) Sign in from a new IP address or a new geographic location not signed in before

e) Sign in behaviours recognized as suspicious after analysed by Central IT or MFA vendors.

5.5 MFA should be adopted for privileged administrative access in an information system.

Reference

The following documents were consulted during the preparation of this document:

City University of Hong Kong (2023), *Information Security Policies*

City University of Hong Kong (2023), *Information Classification and Handling Standard*

Appendix: List of Central IT System Requiring MFA Sign In

The following systems are required to use MFA for sign in:-

a) Administrative Information Management System (AIMS)

b) Remote Desktop Gateway

c) Virtual Private Network (VPN)

d) Microsoft 365

e) Google Workspace

f) CityUHK Pay

g) Privileged Accounts Management (PAM) System

h) Enterprise Content Management (ECM) System