CITY UNIVERSITY OF HONG KONG
Logical Access Control Security Standard

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

Document Control

Document Owner	Classification	Publication Date
OCIO	PUBLIC	2023-01-28

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2015-08-25	Typo corrections
1.2	2023-01-28	Revised the link in this document. Added Multi-factor Authentication (MFA) in section 5 user access management

Distribution

Copy	Issued to	Location
Master	Public	https://www.cityu.edu.hk/cio/information-security/information-security-policies-and-standards

Contents

1 Policy Statement

The City University of Hong Kong ("University") must ensure that the access to the University's information systems, networks, services and resources are controlled on the basis of business and security requirements, and access rights are appropriately authorized, allocated and maintained, and unauthorized access is prohibited.

2 Objective

This document describes the practices of logical access controls employed in the information system operating in the University.

3 Principles

Access to network, systems, applications and information are granted to users on a need-to-know basis, taking into consideration of the business and operation need versus security implication, separation of duties within business processes and classification of information.

For network connectivity or services, the security principle "Everything is generally forbidden unless expressly permitted" shall be considered when granting access.

4 User Identification

Every user will be assigned an Electronic ID ("EID") for accessing IT services provided by the University. EID is a unique lifetime identifier of the user who is the subject of the identity.

Creation of EID must be subject to a formal user registration process.

When new users engage with the University, the corresponding University Unit should provide necessary personal data of new members to Central IT for the EID creation. The creation and activation of EID is invoked by the individual members.

Application for creation of new EID and new secondary account can also be raised by the University Units when new temporary staff or personnel from external service providers come onboard.

5 User Access Management

Access to information shall be managed in accordance to established procedures for the requesting, authorizing, establishing, issuing, suspending, closing, and reviewing user accounts and access rights.

Services owner or controller should set up and maintain role-based access control for the network, systems, applications and information under their administration. Application of privileges should be restricted to addition of roles. Authorization to individual users or request for administrative privileges should be prohibited.

The services owner or controller shall assign, enable, modify, revoke or disable access rights associated with an identity in accordance with the role of identity owner.

Head of Department of new employee or transferred employee should define access rights as soon as the job offer/transfer is confirmed and should verify that the requirements of the roles are aligned with the proposed access rights.

When a change to the access rights of user accounts is required, a formal procedure must be followed.

Rights of granting access to primary information systems/functions were delegated to Heads of Departments, who may assign or revoke access rights to their subordinates as needed.

For the granting of additional access rights, a formal request form must be submitted by the user or user's manager or supervisor to the information systems owner. The request must be approved by user's manager or supervisor and information systems owner before modifying the access rights in information system.

Users shall follow the Password Management and Multi-Factor Authentication Policy and Standards to proper manage and use their passwords and multi-factor login method. On the other hand, user accounts and access rights shall subject to regular review by manager or supervisor of account owner to determine its continued suitability.

6 Network Access Controls

Access to the intranet or Internet will be provided to only those members of the University who have a legitimate need for such access.

All information obtained from the Internet should be confirmed by separate sources. Documents and files downloaded from the Internet shall be scanned with updated anti-virus software before use. Besides, downloaded software should be tested on a stand-alone testing machine. Relevant copyright notice or license agreement regarding the files and software should be observed.

If there is a business need to transmit Central IT information to external parties via the Internet, data user shall follow the Information Labeling and Handling Procedure for the required authorization and protection measures.

Users shall not publicly disclose the University's internal information via the Internet that may adversely affect the University's public image.

Central IT network resources and services shall be segregated into de-militarized zones and internal zones, according to the risks facing by and sensitivity of these resources and services. Properly configured routers and firewalls shall be used to enforce network segmentation, routing and connection controls.

External access to Central IT network resources or services shall subject to user identification, authentication and authorization controls. Appropriate cryptographic techniques should be deployed to protect the information in transit.

External access to administrative, diagnostic or configuration interfaces of network equipment requires stringent user identification and authentication, and shall only be initiated from a trusted location (e.g. IP address and computer name).

7 Operating Systems Access Controls

Users are required to uniquely identify and authenticate themselves to the operating systems (e.g. Windows) via the logon screen, before accessing to applications and information. Password policy of operating systems shall implement the requirements of Password Management Policy and Standards.

After inactive for a pre-defined time period, user sessions should be locked and require re-authentication before continuing.

User access activities should be logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activities by service owner or controller. When necessary, service owner or controller shall consult staff and/or manager or supervisor of staff related to abnormal activities. Access to the log files should be granted based upon the need-to-know basis.

8 Information Systems Access Controls

Users of application systems, including support staff, shall be provided with access to information and application systems based on their need-to-use and individual business application requirements. Sensitive application shall be installed and operated in a dedicated computing environment.

9 Removal of Access Right

The access rights of all employees, students, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment contract, academic program or agreement, or adjusted upon change.

Manager or supervisor of resigned/departed staff or user that initiated the creation of accounts for third party users are responsible for ensuring the timely termination of accounts.

They shall indicate the account validity period when request for creating the account, or send their account termination request to the account administrator of the corresponding service by sending a formal job request before the day of termination.

10 Privilege Management

A privilege is any facility in a multi-user system that enables one user to override system or application controls.

Except those software that are used for business purposes, system utilities and privileged functions that can override system security shall be removed from the information systems.

Privileges are usually identified in terms of user categories (e.g. system administrators) and users are allocated privileges by being joined to user groups that have specific privileges.

The use of privileged functions should be controlled by the following procedures:

- Identify the privileges associated with each system (e.g. operating system, application, database, etc.) and the categories of staff to which these privileges might need to be allocated.
- Allocate privilege on a “need-to-know” and “least privilege” basis and, where possible, event-by-event so that users only have the minimum requirement for their functional role and only for as long as needed.
- Maintain a record of all privileges allocated.
- Set up different accounts, with privileged and non-privilege functions on all information systems or devices.
- Restrict knowledge of the passwords for the system administrator account to the authorized System Administrators only.
- Default passwords for all type of accounts, including general users and administrators, must be changed prior to use in or connecting to production environment.

11 Review of User Access Rights

Principles of the review procedure include:

- Review of normal access rights should be performed at least every twelve (12) months or after any changes in the system.
- Review of privileged access rights should be performed at least every twelve (12) months.
- To perform the review, the Access Control List (“ACL”) of each system is extracted and checked against the current staff list to verify that only currently authorized individuals have system access to perform their job duties.
- The review should be conducted by the management of each department or division of the University. Managers or supervisors should reconcile the ACL against job functions of their staff and formally document the review results.
- The review results University units, and sent to service owner or controller immediately for removal of any inappropriate user account and/or access rights.