CITY UNIVERSITY OF HONG KONG
Human Resource Security Standard

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

PUBLIC **Date of Issue: 2023-01-28**

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	2015-06-19	Typo corrections, and multiple rephrases to improve readability Modified to refer to latest version of “Code of Conduct”, “Guide to CIS” and “Guide to CWS” Replaced “IT Security Officer” with “Information Security Unit”
1.2	2023-01-28	Revised the link and reference material in this document.

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 perform checks to ensure that the individual user is suitable for access to the University's Information Systems and information in these systems. Users are required to sign confidentiality pledge or agreement. Users must be trained, equipped and periodically reminded to use information securely. When employment contracts are terminated, respective user access must be suspended or removed from the Information Systems. When there is a change in role of a user, the information access privileges must be reviewed and changed accordingly on a need to know basis.

2 Objective

The objective of this standard is to govern the human resources aspect of information security for employees of the University.

3 Types of Users

For the purpose of this standard, Employees of the University is anybody who is hired by the University to provide services to the University, regardless of the job function. The following types of staff are usually arranged:

3.1 Full-time, Part-time and Temporary Staff

They are individuals who work in the University as academic, teaching, administrative, general and minor grade staff on full-time, part-time and temporary terms.

All Full-time staff members of the University shall familiarize themselves with their corresponding Staff Handbooks.

For part-time staff, their terms and benefits are in accordance with the provisions of the Employment Ordinance.

For temporary staff, their terms of employment are covered in their Letter of Appointment and the Explanatory Notes attached to the Letter of Appointment.

Students Helpers, who works Campus Internship Scheme (CIS) of the University, is a special type of Part-Time staff or Temporary staff in this regard.

3.2 Contractors and third party users

Instead of being directly employed by the University, they are usually staff of service providers of the University. There are also visitors and guests of the University. If they have to use the University's Information System during the course of their visit or work, they are required to sign a non-disclosure ledge/agreement.

Besides the following guidelines laid down in the Safety and Environmental Protection Handbook for Contractor's Work the same as other contractors working on campus.

4 Prior to Employment / Engagement

4.1 Roles and Responsibilities

All users including information owners and controllers, having specific roles and responsibilities for information security should have documented job descriptions, the terms and conditions of employment or service agreement, which defines these security roles and responsibilities.

4.2 Screening

The procedures for personnel recruitment (including full-time, part-time and temporary staff) should include procedures for appropriate verifications.

Verification checks should, where permitted, include the following:

- Completed Interview Application Form;
- Independent identity checks
- Availability of professional and character suitability references, e.g. from present employer, or academic advisor;
- A check for the completeness and accuracy of the applicants' resumes/application forms and confirmation of claimed academic and professional qualifications;
- Checks of criminal records and credit checks, e.g. bankruptcy, if necessary.

It should be verified that all information related to personal verification checks is handled in accordance with all relevant regulations and legislations. All data collected must only be used for the recruitment purpose and follow the retention policy to dispose information no longer needed.

All application data should be stored in a secured place that can only be accessed by Human Resources Office ("HRO") personnel. Appropriate authorization shall be obtained if transfer of application data is necessary e.g. from HRO to the recommending authority or the prospective University Units of the applicant and follow the retention policy to destroy information no longer needed.

Where persons are supplied by another organization (e.g. secondments or on-site staff of service providers or contractors), the contract with the third party should set out clearly the responsibility of the third party to carry out checks to a similar level, acceptability of person and sub-contracting.

4.3 Terms and Conditions of Employment

The terms and conditions of employment and job description should refer the users to their responsibilities for information security in corresponding job description, handbook and/or guide. The University should make available all security relevant aspects of the job to the employee, including responsibilities applicable to legal requirements, responsibilities related to classified information, working outside the University or outside normal working hours and those responsibilities that might extend beyond the employee's contract.

All staff members of the University shall fully aware of the University's policies and regulations.

> ***Manage Public, Private and Confidential Information Carefully***
>
> *In handling different types of public, private and confidential information, it is staff members' responsibility to:*
>
> - *follow University policies and regulations, and applicable laws regarding collection, access, use, protection, disclosure, retention, and disposal of public, private and confidential information;*
> - *ensure adequate safeguards to prevent abuse or misuse of information; and*
> - *maintain data security.*
>
> *A staff member shall only disclose to other staff members or third party confidential information acquired in the course of employment or University affiliation on a need-to-know basis and only when authorized to do so.*
>
> *The obligation to preserve confidential information continues even after cessation of employment.*

(Sources: City University of Hong Kong Code of Conduct, 3 January 2011 (last updated on 13 November 2020))

Student Helpers shall also be fully aware of the corresponding guide to Campus Work Scheme and Campus Internship Scheme.

> *"During the course of the employment, students are expected to carry out their duties in a diligent manner and not to divulge to outside parties any confidential information concerning the University which may have come to their knowledge."*

(Sources: Guide to Campus Internship Scheme (CIS) version July 2020)

The job descriptions and terms and conditions of employment should also describe the consequence if employees do not fulfill their security responsibilities.

Procedures should be in place to verify that the terms and conditions of employment are updated if the employee's security responsibilities are changed in a way, e.g. taking on new roles or using new or different information processing facilities.

The University's responsibilities for handling personal data of employees, contractors and third party users shall be stated. All users must follow the University's "Personal Data (Privacy) Issues – Code of Practice".

5 During Employment / Engagement

5.1 Information Security Awareness, Education and Training

The University should have some form of induction training, e.g. training course or seminar, web based training, etc., which is given to all employees and contractors and third party users. The induction program is required at general security awareness and technical levels.

5.1.1 Security Awareness Training

Every employee, and where relevant, contractor and third party user, should be given the basic level of security awareness training program. General security awareness sharing sessions for all staff should be organized on a regular basis.

All trainee of the security awareness training program should sit for a quiz before the completion of the training. The objective of the quiz is to help both the University understanding the overall security proficiency of the staff, and help staff understanding their own security proficiency. Staff with result below satisfactory may be requested to attend training and quiz again.

5.1.2 Technical Training

Those staff members with special responsibilities for information security should be provided with necessary skills. A training plan should be developed for each individual in accordance with the specific knowledge and skills required for the position held.

The training organizer should maintain records of training.

The staff shall update records of education, training, skills, experience and qualifications to the HRO.

5.2 Dismissal and Disciplinary Process

The University has standards of behaviour reasonably expected to be maintained by a staff member commensurate with his/her position. Any breach of such standards will be considered as misconduct; disciplinary procedures and actions will be used to deal with such cases.

The University has four different levels of disciplinary actions:

- formal verbal warning
- written warning
- final written warning
- final disciplinary action

Relevant information on dismissal and disciplinary procedures are documented in the following documents:

- Relevant section of respective Service Agreement
- “Dismissal, Disciplinary Procedures and Grievance Procedures” in Staff Handbook applicable to the specific staff
- Regulations Governing Staff Discipline

Any disciplinary actions taken against the employee shall be filed in his/her personal record.

The contract with the third party should set out clearly the University’s right to require changes of any personnel used, engaged or deployed by the contractor or service provider.

6 Termination or Change of Employment

6.1 Responsibilities for Termination or Change of Employment

There should be processes in place verifying that all logical and physical access rights are updated or removed when the job function changes or terminates.

6.2 Change of Employment

HRO should acknowledge the Employees' department as soon as the change of employment is confirmed. Upon confirmation from HRO, the employees' department shall inform the affected managers and supervisors. The original access rights of the employee should be suspended or removed and new access rights should be granted by the manager or supervisor after change.

6.3 Termination of Employment

Employees' department should submit the termination notice or resignation letter to the Human Resources Office as soon as the termination is confirmed. Alternatively, if resignation is submitted to HRO, HRO shall notify Employees' department as soon as the termination is confirmed.

Employee should document knowledge related to current work, and arrange knowledge transfer of the details of the current work.

6.4 Return of Assets

The University has procedures in place to verify that all assets in the possession of employees are returned when their employment terminates or changes.

Employees shall return all of the University's properties such as identity card, cards of benefits, door access card, keys, and any other belongings of the University to the owning University Units upon or prior to the effective date of termination.

Employees shall return assets loan from individual University Units to the owning units.

The cost of any loss or unreturned property of the University will be undertaken by the employee.

6.5 Removal of Access Rights

If an employment terminates, all access rights associated with the employment should be disabled and considered for removal, except some services provided by the University to former staff on a courtesy basis or approved by the responsible service owner or controller.

Upon employment termination, the HRO should provide the relevant staff information to Central IT in order to disable or remove all staff rights associated with the employee.

This includes rights to log into the University's staff network, official e-mail account, software system (if any) and any other form of permitted access.

University Units should also check and take action to either terminate or transfer ownership of role-based accounts and the secondary accounts the staff members involved, or opened based on their job duties.

University Units should also check whether all involved information is properly backed up and the work procedures are being transferred and taken up to avoid loss of information.

The same actions should take place when the employment changes.

7 Responsibilities

7.1 Human Resources Office

- Conduct screening
- Maintain terms and conditions of employment
- Plan and maintain security awareness training with OCIO ISU
- Maintain disciplinary process
- Maintain change of personnel information process
- Notify Central IT and Departmental IT service owners to suspend or remove the logical and physical access rights of employee whose employment is terminated or changed
- Make sure the employee whose employment is terminated or changed returns all non-IT related assets, issued through HRO to the employee

7.2 Central IT and Departmental IT service owners

- Make sure the employee whose employment is terminated or changed returns all IT related assets directly provided by the Central IT or Departmental IT service owners, including the termination of their primary accounts based on the service provisioning policies of the University
- Suspend, remove or transfer of the logical access rights of employee whose employment is terminated or changed based on the requests from the corresponding department

7.3 Information Security Unit (OCIO ISU)

- Work with line managers, head and HRO to allocate roles and responsibilities for information security to employees
- Plan and maintain security awareness training with University Units

7.4 All University Units

- Maintain roles and responsibilities for information security
- Inform the HRO upon resignation or transfer of employees
- Monitor and supervise the employees of his or her department and identify employee who have committed a breach of his or her duties or the University's policies
- Report to the appropriate responsible authority for disciplinary action following the disciplinary procedures of the University
- Make sure the employee whose employment is terminated or changed returns all IT and non-IT related assets
- Transfer ownership of logical and physical IT assets originally allocated by the department to the employees for their job duties and updates the Central IT of such changes

7.5 Employees and third party users

- Comply with relevant Policies, Standards and Terms and Conditions related to employment or service
- Attend the information security awareness training program and complete the related quiz

References

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

City University of Hong Kong (2020), *Code of Conduct*, 3 Jan 2011 (last updated on13 November 2020), https://www.cityu.edu.hk/hro/download/stafflan/admnote/cod_appendix_1.pdf

City University of Hong Kong (2020), *Guide to Campus Internship Scheme (CIS)*, July 2020, https://www.cityu.edu.hk/caio/cis/download/CISGuide.pdf

City University of Hong Kong (2021), *Code of Practice for Personal Data (Privacy) Issues*, Version 18 (Last update:Nov 2021) https://www.cityu.edu.hk/vpad/ctu-only/code-of-practice.pdf