CITY UNIVERSITY OF HONG KONG
Acceptable Usage Standard

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

Document Control

Document Owner	Classification	Publication Date
OCIO	PUBLIC	2023-08-31

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2015-05-27	Multiple rephrases to improve readability. Removed sections that overlapped with the latest version of "Policy on Use of IT Services and Facilities" approved in March 2015, affected sections are: CityU Electronic Mail Regulations Campus IT Network Regulations Electronic University Data Regulations And renumbered sections after the removed sections in version 1.0. Used the term "Computer accounts" Instead "EID", to cover both accounts managed by Central IT and departmental accounts. Clarified that "Clean desk and clean screen standard" only covers "RESTRICTED" and "CONFIDENTIAL" information only, and "INTERNAL" and "PUBLIC" information is not a concern. Modified to allow posting of data to systems "subscribed" by the University, in addition to system owned by the University, to adapt to cloud computing. Allowed the use of "untampered device" to manage "CONFIDENTIAL" or "RESTRICTED" devices, to adopt mobile device and BYOD trend, and further elaborated that "jailbroken", "rooted" are regarded as "tampered".
1.2	2023-01-28	Revised the link in this document. Added Multi-Factor Authentication in section 8 point 3 - Remote access
1.3	2023-08-31	Multiple rephrases to improve readability. Add a section 11 for Generative Artificial Intelligence (GenAI)

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") recognizes the importance of information resources in learning, teaching, research, and administration. Information resources of the University shall only be used for their intended purposes as approved by the University's management and, where personal data is involved, the intended purpose of collection of such data. This standard outlines the specific requirements and guidelines for the implementation of Section 3 – "Acceptable Usage" in "Information Security Policies".

2 Objective

This standard aims to provide guidance, together with formal statements concerning the position of the University, in relation to the use of information resources, which include but are not limited to computer resources, data (in particular personal data), information systems and applications, Internet and intranet, email and instant messaging, social websites, mobile computing devices, portable storage, copyrights and licenses, anti-virus and anti-malicious software, wireless networks and remote access. It also aims to assist staff, students, contractors and third parties in understanding their responsibilities and exercising appropriate judgment when attempting to access these resources.

3 Scope

This standard applies to all users of the University's information resources. Users include members of the University such as staff and students, as well as alumni, retirees, contractors, temporary workers, volunteers and any other third parties who may come into contact with information resources of the University.

4 Principles for Use of Information Resources

"Information resources" include all information and communications technology hardware and software, data and associated methodologies, infrastructure and devices. Refer to Section 3 "Acceptable Usage" of "Information Security Policies" for details.

1. The use of Information resources of the University is a PRIVILEGE, not a RIGHT. Irresponsible use may result in suspension or cancellation of privileges. The University is the final authority to decide whether a user's privileges will be granted, denied or revoked.

2. Users shall abide by the "Policy on Use of IT Services & Resources" while using the University's IT services & facilities operated by Central IT of the University. Users shall also observe the applicable terms & conditions while using services and facilities provided by departments and third parties.

3. Computer accounts are created to facilitate proper user access to information resources. Usually, each user is given a unique account, while shared/team/system accounts may be created for specific purposes. Electronic ID (EID) is a unique identifier assigned to a person based on which computer accounts are created for accessing IT resources managed by Central IT. Departments may use EID and/or department-managed accounts in their systems. The use of information resources should be consistent with the mission of the University.

4. Users are responsible for maintaining the security of their computer accounts and the associated passwords and shall be accountable for all activities performed under their accounts.

5. Users shall safeguard their passwords, change their passwords regularly, log out from systems after use and protect all information resources of the University.

6. Users must use information resources responsibly, reasonably, and legally with the highest integrity.

7. Users must not use information resources for any illegal or unauthorized purposes, such as being engaged in commercial activities for unauthorized personal financial gain.

8. Users must not tamper with the integrity of information resources provided by the University.

9. Users must not attempt to gain unauthorized access to data, information and information resources or disable/circumvent any physical or digital security measures.

10. Users must not develop or use programs to harass other users, infiltrate a computer or computing system within or outside the University, damage or tamper with any components of a computer or computing system, or gain unauthorized access to any services or facilities.

11. Users should use information resources with courtesy and respect.

12. Users should carry out electronic communications (email, web content, forums, etc.) in an ethical and responsible manner and in compliance with general guidelines based on common sense, common decency, and civility applicable to the IT environment

13. Users must not use information resources in a manner that causes or can reasonably be expected to cause, directly or indirectly, unwarranted or unsolicited interference with the activities or work of other users.

14. Users must observe netiquette and any appropriate social conventions in digital communications and must not be engaged in cyber-bullying, trolls and flame wars.

15. User must observe all University's policies, standards and guidelines, as well as all applicable statutory, regulatory and contractual requirements while using information resources of the University.

16. The University reserves the right, without the need for user's prior consent, to monitor the use of information resources, including data (in particular personal data), Internet activities and electronic communications.

17. The University reserves the right, without the need for user's prior consent, to inspect, monitor or disclose any data stored in the University's IT services if there is compelling evidence of any violation of the University's policies or Hong Kong laws, or any normal functioning of the University's IT environment being adversely affected.

18. Failure to comply with this and any IT Policies of the University may result in suspension or termination of some or all IT services provided to a user. Students and staff members may also be subject to disciplinary actions.

19. Users must comply with all applicable laws and regulations when using information resources of the University (See "Compliance Management Standard").

References

https://www.cityu.edu.hk/policies/itpolicy/policies-on-use-of-it-services-and-resources

5 Clear Desk and Clear Screen Standard

It is required that all University information classified as RESTRICTED or CONFIDENTIAL is properly maintained in order to reduce the risks of unauthorized access, loss or damage of such information at all times.

1. Where feasible, paper and other physical media shall be stored in suitable locked cabinets or other forms of secure storage when not in use.

2. In general office, information classified as “CONFIDENTIAL" or above shall be locked away in a fire-resistant safe or cabinet when not in use, especially when the office is unattended. Similarly, notebook computers, personal digital assistants, smartphones, USB devices and other valuable equipment shall be locked away when not in use.

3. For University units where most information would be classified as "CONFIDENTIAL" or “RESTRICTED” and it is impractical to lock away all relevant information, their offices should be protected as restricted areas with receptionists on duty and/or suitable physical entrance control implemented.

4. Personal computers and computer terminals and printers shall not be left logged on when unattended and shall be protected by key locks, passwords, authentication codes or other controls when not in use.

5. Incoming and outgoing mail points and unattended fax machines shall be protected.

6. Photocopiers must be protected from unauthorized use. Outside normal working hours, machine lock or other security arrangement shall be in place.

7. RESTRICTED or CONFIDENTIAL information shall be removed from printers immediately after printing.

8. Licensed software CDs and installation manuals shall be securely stored.

6 Encryption

"CONFIDENTIAL" or "RESTRICTED" information must be encrypted appropriately.

1. Symmetric Encryption:
   When Symmetric Encryption Algorithm is used, the Advanced Encryption Standard with a minimal key length of 128 bits (AES-128) is required, whereas a key length of 256 bits (AES-256) is recommended.

2. Asymmetric Encryption:
   When Asymmetric Encryption Algorithm is used, RSA with a minimal key length of 2048 bits is required.

3. Secure Hashing and Message Digest
   Use of SHA-2 families of secure hashing functions is required for the generation of message digest for the purposes of "Digital signature", "Storage of password" and "Integrity checking"

4. Broken algorithms, e.g. MD5 and SHA-1, must not be used unless necessary for ensuring backward compatibility with legacy systems.

5. Encoding algorithms, e.g. Base64, must not be used as an encryption algorithm.

6. The Information Security Unit of the Office of the Chief Information Officer is responsible for reviewing the appropriateness of encryption and secure-hashing functions annually.

7 Content Sharing Systems and Social Media Systems

Members of the University are using a wide range of Content Sharing Systems and Social Media Systems for communication and collaboration. While these systems may or may not be managed by the University, they are valuable information repositories.

The following applies to all users when using such systems.

1. Only information classified as "PUBLIC" or "INTERNAL" may be posted unencrypted. Please refer to the "Information Classification and Handling Standard" for details about information classifications.

2. Users must encrypt any information classified as "CONFIDENTIAL" or "RESTRICTED" before it is uploaded to these systems. Encryption keys must be distributed through some other channels and must not be stored in the same systems. Users are responsible for the proper key management for the encrypted information to avoid loss and/or unauthorized disclosure of information.

3. Users are required to comply with the terms and conditions of all licensing agreements for copyrighted materials or software. They shall also take reasonable care not to infringe any copyright by uploading or sharing any copyrighted materials or software in breach of licensing agreements.

4. Users should scan all files for malware before uploading and sharing on these systems.

5. Users must not use the systems to access, create, store or transmit materials which may be deemed offensive, indecent or obscene.

6. Unless appropriate prior authorization from the information owner has been obtained, no personal data shall be passed through any University's system/network to any systems which are not owned or subscribed to by the University. Personal information includes, but is not limited to, resume, education credentials, home address, personal identifiers and photographs.

7. Posting of any personal information on the systems must comply with the University's "Personal Data (Privacy) Issues – Code of Practice" and other applicable laws and regulations.

8. The University may, with good cause, delegate the management of a system, in whole or in part, to a unit of the University. Authorized members of such delegated units shall then be responsible for managing the use and access configuration of the systems/sub-system.

9. Users must ensure that all data and information in the systems are secure and up-to-date.

10. The University reserves the right, without any prior consent from users or warning, to prohibit access to, or remove altogether, any data, files or systems that it owns.

8 Remote Access

For enhanced productivity and user experience, remote access to some IT services offered by the University is allowed. Users must make use of such access responsibly.

1. The University's Information Security Policies and Standards, as well as any guidelines, procedures or requirements issued by Central IT or relevant units of the University, are equally applicable to all remote access users.

2. Remote clients are any devices that connect to the University's information resources through an external communication link instead of directly over the campus network.

3. Remote access must be strictly controlled with multi-factor authentication enforced. All passwords and remote access passwords are to be used only by the assigned users and must not be shared. A one-time password should be generated for access to "RESTRICTED" information.

4. Users must not access "INTERNAL", "CONFIDENTIAL" or "RESTRICTED" information from public machines, e.g. public workstations, web cafes, kiosks, etc. Users must not submit their EID and password using these public machines.

5. The University shall make in place appropriate security mechanisms to ensure that remote access connections are secure from interception, eavesdropping or misuse. Some examples of such mechanisms include SSL-VPN and HTTPS.

6. Remote users must not store any downloaded "CONFIDENTIAL" or "RESTRICTED" information in any unencrypted storage.

7. Remote access must be controlled by Central IT. If an external communication link will connect to the campus network, users or departments must register with CSC in advance.

8. Remote users using any remote clients to access the University's information resources must fulfil the following security requirements :

   8.1. Level 1 security requirements

   These requirements apply to users who remotely access "PUBLIC" or "INTERNAL" information resources of the University.

   - Users of a remote client shall normally work with "user" privileges. Full "Administrator" or "Root" privileges can only be used when needed to install software or to make system changes.
   - Latest security patches for firmware and operating systems must be applied and automatic update of security patches must be enabled.
   - Latest security patches for commonly used applications, including but not limited to Adobe Acrobat, Adobe Flash, Chrome, Firefox, Microsoft Office, Internet Explorer and Microsoft Edge, must be applied and automatic update of security patches must be enabled.
   - Screen lock must be enabled

- Password protection must be enabled
- Anti-malware must be installed and running with latest malware definition applied and automatic update of anti-malware and malware definitions must be enabled.

8.2. Level 2 Security requirements

These requirements apply to users who remotely access “CONFIDENTIAL” or “RESTRICTED” information resources of the University.

- Use of a personal firewall if available
- Use of a spyware removal software if available
- Storage encryption enabled for local storage of “CONFIDENTIAL” or “RESTRICTED” information
- Connection to the campus network using an encrypted and secure channel

9 Mobile Device

Users of mobile devices must ensure that effective security measures are in place to protect information resources of the University. This section governs the devices that are owned and managed by the University. The requirement on the acceptable use of private devices is set out in Section 10 “Bring Your Own Device (BYOD)”

Mobile devices are any information processing or storage devices which include, but are not limited to, smartphones, laptops, tablets and desktop computers.

1. Users or owners of devices must diligently protect their devices from loss or disclosure of sensitive or personal information.

2. Access to information resources using mobile devices must comply with the standard for “Remote Access” as set out in Section 8 and, in particular, users of mobile devices must ensure that the configurations of their devices fulfil the “Security requirements for Remote clients” as defined in that Section.

3. Only untampered devices shall be used for accessing University’s information classified as “CONFIDENTIAL” or “RESTRICTED”. Examples of tampered devices include devices which have been "rooted" or "jailbroken", or have any security mechanisms disabled.

4. Security features such as “encrypted storage”, “remote locating” and “remote wiping”, where applicable, must be enabled for devices used for accessing “CONFIDENTIAL” or “RESTRICTED” information.

5. Users of mobile devices should avoid accessing “CONFIDENTIAL” or “RESTRICTED” information in public places.

6. Users must take all reasonable precautions to prevent information disclosure no matter they are on campus, at home or in any remote locations, and are accountable for any information disclosure.

7. Users or owners of mobile devices must report to the University immediately after a device containing “CONFIDENTIAL” or “RESTRICTED” information is lost.

10 Bring Your Own Device (BYOD)

While the practice of "Bring your Own Device" (BYOD) can enhance productivity and user experience, it also poses challenges concerning information security, as well as system management and support. The aim of this BYOD standard is to avoid unauthorized disclosure of sensitive data due to the use of BYOD devices.

The following applies to the use of all "user-owned" devices in accessing any information resources of the University.

1. Users or owners of devices must diligently protect their devices from loss or disclosure of sensitive or personal information.

2. Access to information resources using mobile devices must comply with the standard for "Remote Access" as set out in Section 8 and, in particular, users of mobile devices must ensure that the configurations of their devices fulfil the "Security requirements for Remote clients" as defined in that Section.

3. Only untampered devices shall be used for accessing University's information classified as "CONFIDENTIAL" or "RESTRICTED". Examples of tampered devices include devices which have been "rooted" or "jailbroken", or have any security mechanisms disabled.

4. Users or owners are responsible for the cost and maintenance of their devices and shall contact respective suppliers directly for support services. Central IT and departmental support colleagues can only provide best-effort courtesy support for such devices.

5. To protect against infection or attacks, users or owners must not install on their devices any unsigned or suspicious applications/themes or any peer-to-peer file-sharing software which may access the University's information resources.

6. Users or owners should not enable or establish any Personal Area Network (PAN) using Bluetooth, Infrared or any other technologies, unless absolutely necessary for working or education purposes and with data transmission taking place only between trusted parties. They also should not connect to any ad-hoc Wi-Fi network or any unknown or unsecured network using their devices.

7. If available, users or owners must enable device-level application firewalls for their devices.

8. The University is the ultimate authority to decide whether a device is allowed to access the University's IT services and resources.

9. The University is the ultimate authority to decide whether remote access to any specific information resource, IT service or function provided by an IT service is allowed.

10. The University reserves the right to enforce end-point security on any devices attempting to access its information resources and determine the end-point security requirements. Devices that do not

meet the University's end point security requirements or pass the required end-point security verifications will not be allowed to access any information resources.

11. Users or owners must ensure that the configurations of their devices adhere strictly to the University's security requirements and must not bypass or attempt to bypass any security verifications.

12. The University reserves to right to enable remote wiping on any devices that store data of the University regardless of the ownership of the devices. A device will be remotely wiped if:
    12.1. the device is lost;
    12.2. the University detects any security breach or virus;
    12.3. incorrect passwords are entered from the device for 10 consecutive times

13. Users or owners must report to the University immediately after a device containing University information classified as "CONFIDENTIAL" or "RESTRICTED" is lost.

14. Users or owners shall be fully aware and acknowledge that they will lose all University and personally owned information, including but not limited to personal phonebooks, photos and videos, when their devices are remotely wiped and it is their own responsibility to back up their devices. The University shall not be liable for any consequences whatsoever as a result of such device wiping.

15. At termination of employment, the user/owner of a device is responsible for removing all University's information resources stored in the device.

16. Users or owners who do not follow this BYOD Standard must not use their devices to access the University's information resources.

11 Generative Artificial Intelligence (GenAI)

"Generative Artificial Intelligence" (GenAI) refers to the next generation of artificial intelligence that is designed to be more adaptable, flexible and human-like in its behaviour. The use of GenAI around the world has proliferated rapidly. Seeing its enormous potential, the University encourages, and strives to best facilitate, the proper use of GenAI in all learning, teaching, research and administration.

At the same time, there are also important security considerations when using GenAI. The following applies to the use of general GenAI tools.

1. Users shall ensure that their use of GenAI tools will not result in leakage of sensitive data as user-submitted data may be turned into an AI model's training data and even pop up in the responses to other users. According to the University's Information Security Policies and Standards (ISPS), "User shall not remove or forward RESTRICTED or CONFIDENTIAL information from its premises unless prior approval from the Information Owners/Delegates has been obtained."

2. Users should not download apps or software from any untrusted source, and the use of any downloaded app or software must comply with all applicable legal, regulatory and contractual requirements.

3. Users shall be aware of the risks of copyright infringement when using Gen AI tools to create content and shall avoid using copyrighted materials without permission.

4. Users shall ensure that proper security tools such as Anti-Virus software are installed in their computing environments where GenAI tools will be used.

5. When creating an account for a generative AI tool, users shall always use a strong and unique password that cannot be easily guessed. They should also enable two-factor authentication (if applicable) for their GenAI tool accounts to add an extra layer of security.

6. Users shall ensure their devices, browser and application software are updated regularly to protect against the latest security threats.

CityU offers private instances of pre-trained GenAI services for internal use (i.e. CityU GPT). Users of CityU GPT shall follow the requirements as stipulated in this Standard and the "Policy on Use of IT Services & Facilities".

References

https://www.cityu.edu.hk/policies/itpolicy/policies-on-use-of-it-services-and-resources