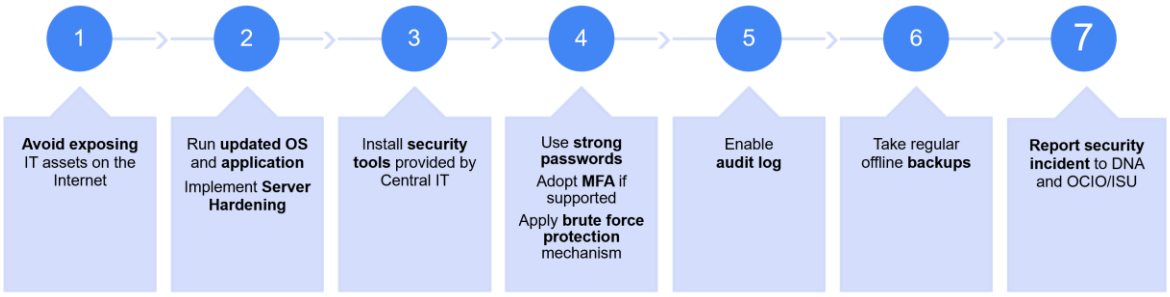
Security Guidelines for Setting Up IT Systems in Academic Departments



1. Avoid exposing IT assets on the Internet

IT assets such as servers, databases, and applications should not be directly accessible from the Internet. This means that they should be placed behind a firewall or other network security device that can filter and block unauthorized access attempts. This reduces the risk of attacks from external sources and helps protect sensitive data and resources.

Staff / Students - If the user requires remote access to the IT asset, please use Central IT Virtual Private Network (VPN)

https://www.cityu.edu.hk/its/services-facilities/virtual-private-network-vpn

Guests/ Collaborators / Supplier – Raise Work Request to request user accounts for guest VPN (gVPN)

2. Run updated OS and application. Implement Server Hardening

Keeping your operating system and applications up-to-date is crucial for security. Updates often contain security patches and bug fixes that address known vulnerabilities.

Server hardening involves configuring your server to minimize its attack surface by disabling unnecessary services, removing default accounts and passwords, and applying security best practices. Server hardening guide can refer to hardening settings such as recommended settings from Center for Internet Security (CIS) https://www.cisecurity.org/cis-benchmarks

3. Install security tools provided by Central IT

Central IT often provides security tools such as antivirus software, firewalls, and intrusion detection/prevention systems that can help protect your IT assets. These tools should be installed, configured, and regularly updated to ensure maximum protection.

- Sophos for Workstation – Contact IT Service Desk for installation
- XDR for All Server and workstations – Contact IT Service Desk for installation
- HIDS for Internet-facing Server – self-services. Fill in survey for license registration
    - Please fill in registration form (https://cityuhk.questionpro.com/t/AUXcEZq1yb – CityU login required) and provide (1) contact person information & (2) server information.
    - Only registered server will be allocated a license. Contact person will be received notification emails related to the server.

4. Use strong passwords. Adopt MFA if supported. Apply brute force protection mechanism

Passwords are the first line of defense against unauthorized access, so it's important to use strong passwords that are difficult to guess. Multi-factor authentication (MFA) adds an extra layer of security by requiring users to provide additional proof of identity beyond just a password. Brute force protection mechanisms can help prevent automated attacks that try to guess passwords by locking out users after a certain number of failed login attempts.

CityU password Policy:

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 age	30 days	the period of time (in days) that a password must be used before the user can 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

https://www.cityu.edu.hk/csc/stafflan/ISMS-ISPS-018_Password_Management_and_MFA_Policy_v1.1.pdf

Brute force protection mechanisms example:

Linux fail2ban -- https://www.linode.com/docs/guides/how-to-use-fail2ban-for-ssh-brute-force-protection/

5. Enable audit log

An audit log is a record of all events that occur on your IT system, including user activity, system changes, and security events. This log can be used to detect suspicious activity, track down the source of a security incident, and ensure compliance with regulations and policies.

Table 4-1. Examples of Logging Configuration Settings

Category	Low Impact Systems	Moderate Impact Systems	High Impact Systems
How long to retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months
How often to rotate logs	Optional (if performed, at least every week or every 25 MB)	Every 6 to 24 hours, or every 2 to 5 MB	Every 15 to 60 minutes, or every 0.5 to 1.0 MB
If the organization requires the system to transfer log data to the log management infrastructure, how frequently that should be done	Every 3 to 24 hours	Every 15 to 60 minutes	At least every 5 minutes
How often log data needs to be analyzed locally (through automated or manual means)	Every 1 to 7 days	Every 12 to 24 hours	At least 6 times a day
Whether log file integrity checking needs to be performed for rotated logs	Optional	Yes	Yes
Whether rotated logs need to be encrypted	Optional	Optional	Yes

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

6. Take regular offline backups

Regular backups are essential for recovering from data loss or corruption caused by hardware failure, software bugs, or cyber-attacks. Offline backups are particularly important because they are not connected to the network, so they are less vulnerable to cyber-attacks such as ransomware.

7. Report security incident to DNA and CSC/ISU

In the event of a security incident, it's important to report it to Department of Network Administrator (DNA) and the Computing Services Centre/Information Security Unit (CSC/ISU). ISU will assist user to handle security incidents and can provide guidance on how to respond to the incident and prevent future incidents.

Prepared by: Information Security Unit (ISU), Computing Services Centre (CSC)

Document Last Update: July 2023