明 志 科 技 大 學

Ming Chi University of Technology

規章編號 Regulation No.
A073090003

公務電腦及可攜式媒體使用規範
Regulations Governing the Use of Official Computers and Portable Media

制定部門：圖書資訊處

Regulatory Agency：Office of Library and Information Services

中華民國 112 年 10 月 31 日修訂

Revised on Oct.31, 2023

修訂記錄：
Revision History:
104.05.19 行政會議編訂
Prepared by Executive Council on May.19, 2015
106.07.25 行政會議修訂
Amended by the Executive Council on Jul.25, 2017
112.10.31 行政會議修訂
Amended by the Executive Council on Oct.31, 2023

目錄

頁次

公務電腦及可攜式媒體使用規範
Regulations Governing the Use of Official Computers and Portable Media

104 年 05 月 19 日行政會議編訂

Prepared by Executive Council on May.19, 2015

106 年 07 月 25 日行政會議修訂

Amended by Executive Council on Jul.25, 2017

112 年 10 月 31 日行政會議修訂

Amended by Executive Council on Oct.31, 2023

第一條 目的

為確保本校教職員正確、安全地操作與使用公務電腦及可攜式媒體，特訂定「公務電腦及可攜式媒體使用規範」(以下簡稱本規範)。

Article 1 Purpose

The Regulations Governing the Use of Official Computers and Portable Media (hereinafter referred to as the Regulations) is hereby formulated to ensure faculties' correct and safe operation and use of the official computers and portable media.

第二條 定義

一、 公務電腦：執行公務使用之個人電腦(含桌上型電腦、可攜式電腦如筆記型電腦或平板電腦)與必要之相關週邊設備。

二、 可攜式儲存媒體：可攜帶並可與電腦連接儲存使用之媒體，包括外接式硬碟或燒錄機、隨身碟、記憶卡、手機、數位相機、平板電腦、磁帶及 MP3/4 Player 等。

Article 2 Definitions

1. Official computers: PCs used for the official business (including desktops, portable computers, such as laptops or tablet PCs) and necessary relevant peripherals.
2. Portable storage media: Media portable or can be connected to the computers for storage and use, including external hard drives or records, flash drives, memory cards, mobile phones, digital cameras, tablet PCs, tapes and MP3/4 Player, etc.

第三條 帳號與密碼管理

一、 應定期更換作業系統登入密碼，每學期至少更換一次。而各應用系統密碼之更換，則配合系統之設定來執行。

二、 密碼複雜度至少 12 碼，且至少須包含英文、數字及符號。

三、 個人應負責保護密碼，維持密碼之機密性。若將密碼記錄在書面上，應妥善保管避免外洩，並且不得將密碼張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。

四、 當有跡象顯示系統及密碼可能遭破解時，應立即更改密碼。

五、 若多人使用同台電腦，應設定不同帳號與密碼登入，以鑑別使用者身分，落實作業安全。

六、 應關閉 Guest 帳號，避免有心人士利用。

七、 禁止與他人共用電腦系統帳號。

八、 管理者權限帳號須限制外部人員登入使用，如有維護設備或其他必要的特殊須求時，須經主管同意後由校內人員陪同下進行。

九、 如有人員職位異動須依規定期限內取消及收繳離職人員於單位內各項資源之權限。

第四條 電腦安全

一、 個人作業電腦應安裝指定之防毒軟體，並定期更新及掃描偵測。進行下載、複製、使用不明來源檔案前，請確認檔案安全無虞，應先完成掃毒，嚴禁任意移除或關閉防毒軟體。

二、 應設定螢幕保護程式及螢幕保護密碼，並將螢幕保護啟動時間設定為 10 分鐘(含)以內，確保人員離開座位時，避免非授權人員作業。

三、 非經授權不得任意使用、拆卸及更動電腦及其週邊設備。

四、 非經授權不得自行重新安裝作業系統，以及刪除作業系統相關日誌檔案。

五、 嚴禁下載、安裝或使用來路不明、有違法疑慮(如版權、智慧財產權等)、未經本校授權或影響本校電腦網路環境安全之軟體。

六、 應定期備份個人電腦設備內重要文件及資訊。

七、 除非業務所必須，個人電腦應儘量避免儲存個人資料檔案；含有大量個人資料檔案應以密碼或加密措施保護。

八、 如非另有公務需求，下班時應將個人使用之電腦關機並將可攜式電腦（如筆記型電腦、平板電腦）收妥。

九、 如非另有特殊需求(如執行特殊應用程式)，同仁應配合進行軟體更新，修補漏洞，保持更新至最新狀態，勿自行關閉系統自動更新程式。

十、 個人電腦如發現資安異常時，應儘速通報電算中心。

十一、 當電腦中毒，病毒無法移除、隔離或作業不正常時，為避免產生大規模電腦病毒感染及擴散情形，應先拔除網路連線，並將電腦關機，通報電算中心。

Article 4 Security of Computer

1. Personal computers should be equipped with the specified anti-virus software, and regularly updated and scanned for detection. Before downloading, copying, or using files from unknown sources, please ensure that the files are secure. File antivirus process should be completed first, and it is strictly prohibited to remove or close antivirus software arbitrarily.
2. The screen saver and screen saver password should be set, and the screen saver startup time should be set within 10 minutes (inclusive) to avoid unauthorized personnel from operating the computer when you're leaving the seat.
3. The computer and its peripherals shall not be used, disassembled or changed without authorization.
4. Do not reinstall the operating system or delete log files related to the operating system without authorization.
5. It is strictly prohibited to download, install, or use software from unknown sources, with illegal concerns (such as copyright, intellectual property rights, etc.), without authorization from our University or that affects the security of our computer network environment.
6. Backup important files and information in personal computer equipment regularly.
7. Personal computers should avoid storing personal data files unless necessary for business; files containing large amount of personal data should be protected with passwords or encrypted.
8. If not for the purpose of official business, turn off personal computers at the end of the day and put away portable computers (such as laptops and tablets).
9. If not for special needs (for example operate special programs), staffs shall cooperate with the software upgrade, patch loopholes, keep updated to the latest state, and do not turn off the automatic system update program.
10. If information security exceptions are found on the computer, please notify the Computer Center as soon as possible.
11. When the computer is attacked by a virus, the virus cannot be removed, the virus cannot be normally isolated, or the normal operation, in order to avoid large-scale computer virus infection and spread, you should first remove the network connection, and shut down the computer, and report the incident to the Computer Center.

第五條 網路連線及作業安全

一、 禁止使用點對點互連(P2P)程式或任何有危害本校網路、設備及造成網路壅塞佔用頻寬等軟體。

二、 瀏覽器安全等級應設定為中級或更高，並關閉快顯功能、ActiveX 等主動執行功能及封鎖彈跳視窗，若執行特殊程式須降低安全性或需加裝外掛功能，應有完整評估。

三、 不得使用即時通訊輸軟體（如 Skype、Line、Yahoo 即時通等）傳輸機密或包含個資之資料，以防止內部之機密件資料及個資遭洩漏。

四、 不得在任何公開之新聞群組、論壇、社群網站或公佈欄中透露任何公務機密相關之細節。

五、 如有架站需求，應遵循本校伺服器管理規範，未經允許，不可任意架站或做私人、營利用途。

六、 非經授權，禁止使用密碼破解、網路竊聽等工具軟體，且不得突破他人帳號、中斷系統服務、濫用系統資源及複製非法軟體。

七、 同仁應避免使用非本校防護範圍內之網路及電腦設施來辦理公務，若確有必要使用外部(如住家、公共場所)資訊環境，務請確認資訊使用環境是否具備下列防護措施：

1. 若需連線回校內網站或是公務電腦作業，需透過具備加密之軟體或利用本校虛擬私有網路(VPN)連線作業，確保資料傳輸安全。
2. 儲存於可攜式儲存媒體之公務相關電子檔案應予加密。
3. 使用之連網電腦設備應安裝防毒軟體(含最新版之病毒碼更新)及防火牆，並應保持啟動運作狀態。
4. 於處理完畢後應將公務相關電子檔案移除，且不得存放於主機。
5. 如使用學校網路或本校提供之宿舍網路連線，除了本項第一款外，其餘應遵循。

八、 各單位如建立網路儲存系統(NAS)進行資料備份或儲存作業，則應設定內部虛擬 IP，並且遵循本規範第四條與第五條所提事項，確保資料安全。

九、 若開啟網路分享，須設定密碼及可存取之帳號，嚴格控管電腦分享資料存取。

十、 如使用網路公告或交換資訊，應評估資料安全等級，不得於網路上洩漏未經當事人同意之個人隱私、機密或敏感資料及文件。

Article 5　Network Connection and Operation Security

1. It is forbidden to use peer-to-peer (P2P) programs or any software that may harm the University's network, equipment, or cause network congestion to occupy bandwidth.
2. Set the security level of the browser to medium or higher, and disable active execution functions such as flash display and ActiveX, as well as block pop-up windows. If special procedures require reduced safety or add-ons, a complete evaluation should be conducted.
3. Do not use real-time communication software (such as Skype, Line, Yahoo, etc.) to transmit confidential or personal information to prevent internal confidential information and personal information from being leaked.
4. Do not disclose any details related to official secrets in any public news group, forum, social networking site or bulletin board.
5. If you need to set up a website, you should follow the University's server management regulations. Without permission, you are not allowed to set up any website or do private or commercial purposes.
6. Do not use tools and software such as password cracking and network eavesdropping without authorization, and do not crack others' accounts, interrupt system services, abuse system resources, or copy illegal software.
7. Employees should avoid using networks and computers that are not within the protection scope of the school for official business. If it is necessary to use external information environments (such as homes or public places), please confirm whether the information usage environment has the following protective measures:
    1. If you need to connect to the campus website or work on official computers, you must use encrypted software or use the University's virtual private network (VPN) to ensure the security of data transmission.
    2. Electronic records related to official business stored in portable storage media shall be encrypted.
    3. The connected computer equipment used should be installed with anti-virus software (including the latest version of the virus pattern update) and firewall, and should be kept in the running state.
    4. After the processing is completed, the electronic files related to official affairs should be removed and should not be stored in the host.

5. If you use the campus network or the dormitory network provided by the University, the rest shall be followed except for item 1 of this paragraph.

8. If each unit establishes a NAS for data backup or storage, it should set up an internal virtual IP and follow the matters mentioned in Articles 4 and 5 of the Regulations to ensure data security.
9. If you enable network sharing, you must set a password and an accessible account to strictly control the access of computer sharing data.
10. If you announce or exchange information on the Internet, you should assess the level of data security, and you should not disclose personal, confidential or sensitive information and documents on the Internet without the consent of the parties.

第六條 電子郵件使用安全

一、 電子郵件附加之檔案，應事前檢視內容無誤後方可傳送。

二、 電子郵件宜設定純文字閱讀，或是關閉郵件預覽功能及圖片自動下載功能，且不開啟來路不明之電子郵件及其附件，以免感染惡意程式。

三、 為配合教育部電子郵件社交工程演練，本校得由圖書資訊處電算中心辦理內部電子郵件社交工程演練。而演練期程、主題內容及演練對象由圖書資訊處電算中心另訂，演練不合格人員需配合調整電子郵件相關參數。

四、 不得使用校外網頁式電子郵件傳輸個人隱私、機密或敏感資料檔案。

五、 電子郵件傳送個人隱私、機密或敏感資料時，須以適當的加密或電子簽章等安全技術處理。

Article 6 Email Use Security

1. The file attached to the E-mail should be checked in advance before it can be transmitted.
2. It is advisable to set the email to be read in plain text, or turn off the email preview function and automatic image download function, and do not open emails and attachments from unknown sources to avoid infecting malicious programs.
3. In order to cooperate with the E-mail social engineering drill of the Ministry of Education, the University may request the Computer Center of the Book Information Office to conduct an internal E-mail social engineering drill. The drill schedule, subject content and drill object shall be set separately by the Computer Center of the Book Information Office, and if a person fails the drill, he/she shall cooperate in adjusting email

parameters.

4. Do not transmit personal, confidential or sensitive information files with off-campus web-based email.
5. When sending personal, confidential or sensitive information by E-mail, it shall be handled with appropriate security techniques such as encryption or electronic signature.

第七條 儲存媒體、可攜式資訊設備及其它存取裝置使用安全

一、 使用可攜式儲存媒體儲存機密性、敏感性或個人隱私資料時，宜先取得授權並予加密保護。

二、 應避免使用私人移動裝置存取公務，如需使用私人移動裝置存取公務資料，應遵守本規範第五條之規則，並且禁止存取機敏性資料。

三、 廠商或其他單位以可攜式儲存媒體交付資料時，須先對檔案進行病毒掃描，確認無惡意軟體之威脅。

四、 對於可重複讀寫之儲存媒體，執行資料儲存前其儲存媒體應清空，內容僅含須交付之資料。

五、 應妥善保管可攜式資訊設備與儲存媒體，避免遭竊或未授權使用。

六、 可攜式資訊設備或儲存媒體若為共用時，設備歸還管理人（負責人）時，應檢查確認可攜式資訊設備已維持淨空或原貌，僅保留共用之應用程式及軟體，避免資料遭未授權存取或誤用。

七、 燒錄完成之光碟片或磁帶應完整標示機密等級與檔案內容，避免遭誤用。

八、 可攜式資訊設備或儲存儲存媒體若有故障需送外部維修時，該資產所有人（負責人）應確保電腦內不含機敏性資料，或是確保機敏性資料不會外洩。

九、 欲報廢之儲存媒體(包含電腦等資訊設備內含之儲存裝置)，若有含機敏資料，如：個資、有效授權之軟體等，應將儲存資訊刪除，如為硬碟、磁帶、隨身碟等儲存裝置，應填寫「儲存媒體銷毀抹除申請單」(表號：A073090103)，送交主管簽核後，將儲存裝置及申請單交由電算中心審核無誤後，自行操作硬碟抹除機或破壞機進行抹除或銷毀至無法解讀之程度後方能辦理資產閒置。若為光碟片，則由當事人直接銷毀至無法解讀之程度。

十、 如存放公務資料之儲存媒體、可攜式資訊設備或其它存取裝置遺失，應依照本校急要事件處理程序進行通報作業，以追蹤及控管風險。

Article 7 Use Security of Storage Media, Portable Information Devices and Other Access Equipment

1. When storing confidential, sensitive or personal data with portable storage media, it is advisable to obtain authorization and encrypt it.
2. Avoid using private mobile devices to access official information. If private mobile devices are used to access official information, the provisions of Article 5 of this Regulations shall be observed, and the access to sensitive information shall be prohibited.
3. When delivering data on portable storage media, manufacturers or other organizations must first scan the files to confirm that there is no threat of malware.
4. For rewritable storage media, the storage media shall be emptied before data storage is performed, and the content shall only be about the data to be delivered.
5. Keep portable information equipment and storage media safe from theft or unauthorized use.
6. When the shared portable information device or storage media is returned to the manager (person-in-charge), it shall be checked to ensure that the portable information device has been kept clear or in its original condition, and only the shared applications and software are retained to avoid unauthorized access or misuse of the data.
7. The burned disc or tape should be fully marked with the confidential level and file content to avoid misuse.
8. If there is a malfunction in portable information devices or storage media that requires external repair, the owner (person-in-charge) of the asset should ensure that the computer does not contain sensitive information or that sensitive information is not leaked.
9. If the storage media (including the storage devices embedded in the information equipment, such as computers) to be scrapped contains sensitive information, such as: personal information, valid authorized software, etc., the storage information should be deleted. In case of the storage devices of hard drive, tape, flash drive, etc., the “Application Form of Destruction and Erasure of Storage Media” (Form No. A073090203) shall be filled in and submitted to the supervisor for signature and approval before sending the storage devices and application form to the Computer Center. After they are reviewed to be right and correct, operate the hard disk eraser or destructor to erase or destroy the storage

device or application until it is unreadable. If it is a CD, it shall be destroyed directly by the users to the extent that it cannot be interpreted.

10. In case of loss of storage media, portable information devices or other access devices that store official data, the school shall report the loss in accordance with the emergency handling procedure to track and control the risk.

第八條 教育訓練及宣導

一、 為增進教職員資訊安全之觀念，資訊委員會應定期辦理資訊安全教育訓練，增進人員認知。

二、 資訊委員會應不定期進行資訊安全宣導作業，提醒教職員遵循規範。

Article 8 Education, Training and Advocacy

1. In order to enhance the concept of information security of faculties, the Information Committee shall conduct information security education and training on a regular basis to enhance staffs' awareness.
2. The Information Committee shall conduct information security advocacy from time to time to remind staff to follow the Regulations.

第九條 稽核作業及事件通報

一、 圖書資訊處配合個人資料保護稽核作業時，進行公務電腦稽核。如有特殊狀況需進行專案稽核，則需獲得校長或被查核單位之一級主管同意方得執行。

二、 如有必要，可邀請校內同仁或校外專業人員協助稽核。

三、 稽核人員可利用各項軟體工具及控管系統相關資料來進行稽核作業(如密碼破解軟體、網路監聽等工具)，但須於稽核計畫或會議提出，經稽核小組召集人同意。

四、 本校教職員需配合稽核作業，如有不配合，則中斷稽核作業並於稽核報告內，列為重大缺失。

五、 稽核有所爭議，由稽核小組召集人開會討論處理。

六、 如發生資安事件(包含設備遺失、資料外洩或系統入侵…等)，當事人應依照本校資安事件處理程序進行通報作業，以追蹤及控管風險。

Article 9 Audit and Incidents Report

1. When protecting and auditing the personal information, the Office of Library and Information Services shall carry out the audit on official computers. For special situation requiring project audit, the consent from President, or Superior

Supervisor of the audited unit shall be obtained before the audit.

2. Invite on-campus colleagues or off-campus professionals to assist in the audit if necessary.
3. The auditor may audit with all kinds of software, tools and control system as well as relevant materials (such as password cracking software, network monitor, etc.) on the premise that he/she shall propose on the audit plan or at the meeting and obtain the consent from the convener of audit group.
4. The faculties of the University shall cooperate with the audit. If they fail to cooperate, their behavior shall be indicated as major deficiency in the audit report.
5. Any disputes over the audit shall be subject to discussion at the meeting convened by the convener of the Audit Group.
6. In case of information security incidents (including device loss, data leakage or system intrusion, etc.) the party involved shall notify in accordance with the processing procedures for the information security incidents of the University to track and control risks.

第十條 實施與修訂

本規範經行政會議通過，陳請校長核定後公佈實施，修訂時亦同。

Article 10 Implementation and Amendments

The Directions shall be passed by the Executive Council and will be enacted and become effective after the approval of the principal. The same shall apply to any amendments to the Procedures.

儲存媒體銷毀/抹除申請單

申請單位		申請單號	20231113-經辦工號末五碼+2 碼流水號
申請人		申請原因	□資產移轉　□資產減損　□資產閒置

儲存媒體基本資料				
資產編號	媒體廠牌	媒體序號	媒體狀態	處理方式
			□正常□無利用價值□壞軌	□完整抹除□DOD 抹除□七次抹除□銷毀破壞
			□正常□無利用價值□壞軌	□完整抹除□DOD 抹除□七次抹除□銷毀破壞
			□正常□無利用價值□壞軌	□完整抹除□DOD 抹除□七次抹除□銷毀破壞
			□正常□無利用價值□壞軌	□完整抹除□DOD 抹除□七次抹除□銷毀破壞
			□正常□無利用價值□壞軌	□完整抹除□DOD 抹除□七次抹除□銷毀破壞
			□正常□無利用價值□壞軌	□完整抹除□DOD 抹除□七次抹除□銷毀破壞
			□正常□無利用價值□壞軌	□完整抹除□DOD 抹除□七次抹除□銷毀破壞
			□正常□無利用價值□壞軌	□完整抹除□DOD 抹除□七次抹除□銷毀破壞
			□正常□無利用價值□壞軌	□完整抹除□DOD 抹除□七次抹除□銷毀破壞

電算中心經辦	媒體銷毀/抹除經辦	主管	組長	申請人

處理方式說明：
完整抹除：將整個硬碟磁區都填入 0 或 1，包含空白區域
DOD 抹除：符合美國 DoD5220.22 抹除，連續執行三次完整抹除，第一次填入 00 值，第二次填入 FF 值，第三次則是填入亂數
七次抹除：符合美國 DoD5220.22 抹除，連續執行七次完整抹除，第一、五次填入 00 值，第二、六次填入 FF 值，第三、四、七次則是填入亂數
銷毀破壞：以硬碟破壞機，進行實體打洞破壞

表號：A073090103

Application Form of Destruction and Erasure of Storage Media

Applying Unit		Application Form No.	20231113-five codes of undertaking numbers+2 codes of serial numbers
Applicant		Reason for Application	□asset transfer □asset impairment □ asset idleness

Basic Information of Storage Media

Asset No.	Media Brands	Media Serial No.	Media Status	Processing Method
			□normal □useless □bad sector	□completely erased □DOD erased □erased for 7 times □destroyed
			□normal □useless □bad sector	□completely erased □DOD erased □erased for 7 times □destroyed
			□normal □useless □bad sector	□completely erased □DOD erased □erased for 7 times □destroyed
			□normal □useless □bad sector	□completely erased □DOD erased □erased for 7 times □destroyed
			□normal □useless □bad sector	□completely erased □DOD erased □erased for 7 times □destroyed

Undertaken by the Computer Center	Undertake to destroy/erase the media	Supervisor	Group leader	Applicant

Descriptions of Processing Method:
Completely erased: Fill the entire hard drive area with 0 or 1, including blank areas
DOD erased: Conforms to the US DoD5220.22 erasure, completely erased three times in a row. With 00 filled in for the first time, FF filled for the second time and any number for the third time.
erased for 7 times: Conform to US DoD5220.22 erasure, completed erased seven times in a row, with 00 filled in for the first and fifth time, FF filled for the second and sixth time and any number for the third, fourth and seventh time.
Destroyed: Destroyed the media with hard drive destructor by making a hole on it.

Form No.: A073090203