長 庚 大 學

規章編號
0400003

資訊安全管理辦法

訂定部門：資訊中心

中華民國 98 年 9 月 10 日訂定

中華民國 113 年 3 月 26 日修正

訂定(修正)記錄：
98年9月10日行政會議通過訂定
103年2月27日行政會議通過修正
105年5月12日行政會議通過修正
106年11月16日行政會議通過修正
112年1月10日行政會議通過修正
113年3月26日行政會議通過修正

長庚大學資訊安全管理辦法

98年3月12日行政會議通過訂定
113年3月26日行政會議通過修正

第一條 目的

長庚大學（以下簡稱本校）為強化資訊安全管理，督促改善資訊安全防護，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，特訂定「長庚大學資訊安全管理辦法」(以下簡稱本辦法)。

第二條 適用範圍

本校各項資訊資產使用者，含全校教職員生、合約廠商駐校人員及其它經授權使用之人員。

第三條 組織與權責

一、為強化本校資訊安全，健全資訊安全管理制度，特設立「長庚大學資訊安全委員會」(以下簡稱本委員會)，以推動本校資訊安全管理業務之運作。

二、本委員會設置委員二十至三十人，由主任秘書以上擔任資訊安全長並兼任本委員會召集人，資訊中心主任為執行秘書。當然委員包括教務長、學務長、總務長、研發長、技合長、國際長、永續長、人事室主任、會計室主任、環安室主任、體育室主任、圖書館館長、文物館館長、各學院院長、通識教育中心主任及各校級研究中心主任，其餘委員由本委員會召集人就本校業務相關主管或具資訊相關專長之教職員中遴選。委員為無給職，聘期二年，期滿得續聘。

三、本委員會權責如下:

1. 訂定本校資訊安全政策及資訊安全管控機制。
2. 督導資訊安全政策之實施。
3. 資訊安全事件通報、緊急應變及危機處理。
4. 規劃並督導資訊安全教育訓練及其他資訊安全相關事項。
5. 協助推動本校資訊安全管理系統之認證。

四、本委員會每學年開會一次為原則，得視業務需要召開臨時會議。

會議須有應出席委員半數(含)以上出席始得開會，並得邀請相關人員列席。

第四條 電腦系統安全防護

一、 所有電腦帳號須設定密碼，訪客等公用帳號須停用，使用者須善盡帳號密碼保管之責，並定期更換。

二、 各類作業系統若有螢幕保護功能，必須啟用。啟動螢幕保護時間設定應小於十分鐘，且須設定繼續後以密碼保護功能。

三、 各類作業系統及應用軟體須開啟自動更新功能或留意其更新資訊，隨時確保軟體的漏洞為已修補狀態。電腦因故重灌後，應立即重新完成所有之漏洞修補作業。

四、 所有電腦必須安裝防毒軟體，不可任意關閉或移除，且防毒軟體病毒碼須定期更新。若因應教學管理需要不安裝防毒軟體應有其他措施進行防護。

五、 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，應將電腦關機，並拔除網路連線，並通報資訊中心。

六、 來路不明的軟體或檔案常為散播病毒的來源，為確保電腦使用安全，不得安裝使用。

七、 電腦系統若具備防火牆功能，必須開啟，以提升電腦防護能力。

八、 各單位架設伺服器依照本校「校園伺服器管理辦法」，須有專人負責維護並進行相關資訊安全作業。

九、 禁止與他人共用電腦系統帳號。

十、 採取權限區隔，非專責處理特定機密或敏感資料者，不得具有存取或查閱機密或敏感資料之權限。

十一、 禁止人員使用即時通訊軟體傳輸機密或敏感資料檔案。

十二、 禁止人員使用校外網頁式電子郵件傳輸機密或敏感資料檔案。

十三、 禁止人員使用點對點（P2P）軟體及即時通訊軟體等相關工具下載或提供分享檔案。

十四、 禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之機密或敏感資料。

第五條 存取控管

一、 各單位利用網路公佈及流通資訊時，應評估資料安全等級，未經當事人同意之機密或敏感資料及文件，不得上網公佈。

二、 機密或敏感資料及文件，欲利用電子郵件傳送時，須以適當的加密或電子簽章等安全技術處理。

三、 電腦內的資料若須開啟網路分享，務必設定密碼及可存取之帳號，嚴禁未設權限控管開放電腦資料供人任意存取之行為，以防電腦病毒侵害及機密或敏感資料洩露或損毀，且重要資料務必定期備份。

四、 各單位離職人員須依規定期限內取消使用單位內各項資源之所有權限，並列入人員離職之必要手續。

五、 各單位主機須限制外部人員以管理者權限帳號登入使用，如有設備保管人以外人士使用或維護設備的須求時，須經主管同意後由系統管理人員陪同下進行。

六、 應指定專人負責管理儲存機密或敏感資料檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息。

七、 儲存機密或敏感資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。

八、 儲存機密或敏感資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境(如：上鎖之防潮箱、書櫃)，必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。

九、 儲存機密或敏感資料檔案之電腦或相關設備如須報廢或移轉他用時，應確實刪除該設備所儲存之機密或敏感資料檔案。

十、 對重要資訊服務之日誌與紀錄等加以適度存檔，以便日後查核使用。

第六條 可攜式儲存媒體

一、 使用可攜式設備，須先確認電腦已安裝啟用防毒軟體，避免電腦、系統與網路受到病毒威脅。

二、 使用可攜式設備與媒體時，須謹慎防範資訊洩漏或妨害本校利益等情節發生，資料攜入或攜出，使用者單位主管或廠商接洽窗口人員須盡控管之責。

三、 將機密或敏感資料存放於可攜式設備與媒體時，須採取適當加密處理或保護措施，避免遺失時洩漏資訊。

第七條 實體與安全環境管理

一、 外部人員及訪客須遵守各單位辦公區域安全管制相關規定，並於指定環境內執行作業，防止未經授權的存取、干擾及損害。

二、 重要之出入口須有門禁管理機制，內部人員於進出時須隨時注意是否有非經授權人員跟隨進入，保持警覺，留意陌生人士。

三、 使用影印機、印表機、傳真機或多功能事務機等資料複印設備後，須立即將相關資料取走，並清除可能暫存於該設備之資訊。

四、 機密或敏感資料須放置於抽屜或儲櫃並上鎖。

五、 下班時，必須實施桌面淨空，重要文件妥善保管，並關閉不須使用之電腦系統暨其週邊設備。

第八條 資安教育訓練與宣導

本校人員須定期參與資訊中心主辦的資訊安全教育訓練及宣導，建立並加強資訊安全認知，提升資訊安全水準。

第九條 人員管理

一、 各單位對資訊相關職務及工作，須進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

二、 各單位對負責重要資訊系統管理、維護、設計及操作之人員，須妥適分工，分散權責，並視須要建立制衡機制，實施人員輪調，建立人力備援制度。

三、 本校各級業務主管人員，須負責督導所屬員工之資訊作業安全，防範不法及不當行為。若有違反，由主管單位送請校方依本校相關法規懲處。

四、 處理機密或敏感資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置密碼外，應視須要更換使用者識別帳號。

五、 處理機密或敏感資料檔案之人員，應簽訂保密切結書，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。

第十條 資安事件通報

一、 校內人員若發現有資訊安全可疑事件時，須儘速通報資訊中心。資訊中心做緊急必要之處理後會發出「資訊安全事件處理暨回覆單」給事件發生單位，事件發生單位須填寫後續處置情形,經主管核簽後回覆資訊中心存查。

二、 各單位須設資安聯絡人及其職務代理人，負責資安事件之通報及處理等業務，並將名單送資訊中心存查。

第十一條 系統開發及委外管理

一、 自行開發或委外處理機密或敏感資料檔案之資訊系統，應在系統開發生命週期之初始階段，將機密或敏感資料檔案的安全須求納入考量(如:邏輯測試);系統之維護、更新、上線及版本異動等作業，應予安全管制，避免危害機密或敏感資料安全。

二、 維護人員或系統服務廠商避免以遠端登入方式進行牽涉機密或敏感資料的資訊系統維護或其他有關之運作；若因業務須要必須使用遠端登入方式進行維護時，應透過加密通道進行（如：HTTPS、SSH 等）。

三、 自行開發或委外處理機密或敏感資料檔案之資訊系統，應將機密或敏感資料施予妥善之保護與控管。

四、 機密或敏感資料檔案若委外建檔，應於委外合約中載明所處理之機密或敏感資料保密義務、資訊安全相關責任及違反之罰則。

五、 透過網路存取之相關系統應於上線前，確認所開發的系統架構是否已排除系統安全弱點之漏洞。

第十二條　施行與修正

本辦法經行政會議通過，陳請校長核定後公布施行，修正時亦同。