

# 嶺東科技大學資訊設備暨網路安全管理作業要點

103 年 12 月 24 日 103 學年度第 1 學期第 6 次行政會議通過

108 年 08 月 19 日 108 學年度第 1 學期第 1 次行政會議通過

## 一、目的

嶺東科技大學（以下簡稱本校）為落實「個人資料保護法」及資訊安全管理制度等相關規定，確保本校機密性及敏感性資料、作業系統、資訊設備、網路及資訊業務委外等內容納入安全管理，特訂定「嶺東科技大學資訊設備暨網路安全管理作業要點」（以下簡稱本要點）。

## 二、機密性及敏感性資料安全管理

- (一) 機密資料應依相關規定，明確標示機密屬性、等級及保密期限。
- (二) 重要資料檔案應以安全之方式保存，以防止遺失、毀壞、被偽造或竄改。
- (三) 儲存機密性及敏感性資料之電腦媒體，不再繼續使用時，應以安全之方式處理（如：消磁、上鎖等）。
- (四) 各單位間進行資料交換，應考量機密或敏感性資料之安全保護措施（如：資料加密等）。

## 三、作業系統安全管理

- (一) 作業系統應安裝防毒軟體，隨時更新病毒碼，並下載系統漏洞修補程式。
- (二) 各單位應使用合法版權軟體進行資訊作業。
- (三) 單位內部作業系統應依人事組織改變，進行使用者帳號存取權限調整。
- (四) 本校員工職務異動、離職時，人事單位應通知資訊網路中心，變更人員帳號權限。

## 四、資訊設備安全管理

- (一) 依本校資訊安全管理制度規範，應建立資訊設備清冊、管理人及安全等級分類。
- (二) 含有儲存媒體的資訊設備，應在報廢處理前詳加檢查，以確保機密性資料及有版權之軟體已被移除。
- (三) 資訊設備應由專人負責管理，定期維護保養，以確保設備之可用性。
- (四) 重要資訊設備存置場所（如：IDC 機房），應設置消防系統、緊急供電系統、門禁安全控管及各式天災防護措施，並定期接受資訊安全稽核，以確保資訊作業安全。

## 五、網路安全管理

- (一) 本校須設置專責之網路管理者，負責網路資源管理及檢閱網路安全有關紀錄。
- (二) 禁止下載或使用來路不明、未經授權或影響電腦網路環境安全之電腦軟體。
- (三) 禁止使用點對點軟體進行下載或提供分享檔案。
- (四) 因教學、研究或行政作業上需求，欲申請對外開放網站連接埠，須經申請審核。
- (五) 發生網站入侵危安事件，應依資安通報流程逕行通報。

## 六、資訊業務委外安全管理

下列有關資訊安全之事項，應納入資訊業務委外之服務契約內容中：

- (一) 涉及機密性、敏感性或關鍵性之應用系統項目。
- (二) 應經核准始得執行之事項。
- (三) 應遵守本校資訊安全規範，配合進行資訊安全評估及營運持續計畫演練。
- (四) 應處理及通報資訊安全（包括違反「個人資料保護法」）事件之責任。
- (五) 應於簽訂契約時同時簽署保密切結書。

七、本要點負責單位為圖書資訊處資訊網路中心，上述各事項由該中心依權責辦理。

八、本要點經行政會議通過，陳請校長核定後實施，修正時亦同。