# 台鋼學校財團法人台鋼科技大學電腦安全管理作業規範

103 年 12 月 8 日資訊安全委員會通過
103 年 12 月 9 日行政會議通過
108 年 8 月 27 日行政會議通過
111 年 12 月 6 日行政會議通過
113 年 3 月 26 日行政會議通過

第一條　目的

台鋼學校財團法人台鋼科技大學(以下簡稱本校)依據教育部台電字第 0960196582 號函辦理制定「台鋼學校財團法人台鋼科技大學電腦設備安全管理作業規範」(以下簡稱本規範),加強督促改善校內之資訊安全防護,避免因人為疏失、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,而影響電腦系統正常運轉。

第二條　適用範圍

一、人員:本校在職之教、職員工(含約聘僱人員)、學生等使用本校資訊資源,或資訊業務委外服務之廠商人員。
二、資訊作業:各類個人電腦、工作站、主機、伺服器、系統等(以下簡稱資訊作業)。

第三條　管理及權責

一、圖書資訊中心(以下簡稱本中心)為本校資訊作業安全管理之督導單位。
二、各單位為業務用資訊作業之使用單位,實際負責單位內資訊作業之安全保護事宜。

第四條　人員安全管理與資訊安全教育訓練

一、各單位主管應負責督導所屬教職員工之資訊作業安全,防範不法及不當行為。本校教、職員工(含約聘僱人員、計畫人員) 、學生等,必須遵守本規範。
二、本校資訊業務,若有委外服務之廠商人員,應於簽訂契約時,同時簽署廠商及人員保密切結書,切結遵守本規範。
三、本校人員須參與本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。
四、各單位重要系統之管理、維護、設計及操作,應建立人力備援機制。
五、如因職務異動成為非授權使用者時,隸屬單位應主動通知各單位更改使用者密碼或刪除該使用者帳號。
六、各單位人員離職時,須依規定辦理離職手續,並終止相關資源之存取權限,確實做好電腦軟硬體及相關文件之移交工作。
七、違反本規範者,將依本校教職員工獎懲辦法查處。

第五條　電腦系統安全管理

一、資料庫或個人重要資料應定時執行備份,並異地存放,以確保資料的安全。
二、處理含個人資料時,應依據「個人資料保護法」及相關規定審慎處理,不得私自蒐集或洩漏業務資訊,非依法不得調閱使用。
三、各單位之個人資料索取或調閱,依據「個人資料保護法」及相關規定審查後,始可提供資料。

四、需使用合法版權軟體，避免上網下載使用來路不明軟體。

五、與外部交換機密敏感資料時，需依據安全查核機制，確定無安全疑慮，方可進行。

第六條　系統存取控制

一、因執行業務及職務所必要時，得賦予使用者適當的系統存取權限。但工作調整時，使用者名稱須立即異動。

二、應用系統使用者，需擁有各自的使用者名稱和密碼，不可多人使用同一組帳號密碼；不同的使用者，各有不同的作業範圍和權限。密碼必須加以保密，避免洩密遭人盜用，並應定期六個月更改通行密碼。

三、人員因故離開座位暫停作業時，必須登出系統或使用畫面鎖定保護，防止帳號被盜用或資料被竊取。

四、重要資料異動時需簽核至校長，於校長核准後始得修改資料。資料庫資料修改時，須由資料庫管理者登入修改，並需會同系統管理者、組長及本中心中心主任在場。

第七條　資訊資產之安全管理

一、建立資訊系統有關資訊資產目錄，明列資訊資產的項目、管理（負責）人及安全等級分類，如有變更應詳細記載。

二、分類依據國家機密保護、個人資料保護及政府資訊公開等相關法規，區分為機密、敏感、限閱、一般等四類。

三、資訊作業實體設備故障應通知資產管理（負責）人，並由管理（負責）人依規定提出請修申請。

四、資訊資產實體設備報廢，由財產管理人員依規定辦理。

五、含有儲存媒體的設備，應在報廢處理前詳加檢查，以確保機密性、敏感性之資料及有版權之軟體已被移除。

第八條　資訊業務委外之安全管理

一、委外作業廠商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。

二、委外作業廠商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。

三、資訊業務委外時，應於事前審慎評估可能的潛在安全風險，並與廠商簽定適當的資訊安全協定，及課以相關的安全管理責任，納入契約條款，必要時並應不定期派員監督、管理委外廠商實際作業情形。

四、委外作業承包之工作人員，如需進入相關系統作業應經核准始得執行。由委外業務之主管單位依規定申請使用者帳號,並於委外業務完成後立刻依規定刪除。

五、委外作業輸入之資料由主管單位指派專人核對以確保資料之正確性，委外資訊廠商除安全管理責任外，尚應落實保密作為。

六、系統委外開發承包商應提供系統建置（含規格及軟體程式）之完整、詳細說明文件。

第九條　實體及環境安全管理

一、資訊設備安全管理

(一) 專人負責，並制訂資訊設備開關機操作程序。

(二) 應定期維護保養，確保設備的完整性及可以持續使用。

(三) 資訊設備、資料或軟體，未經管理人員同意下，不得攜離辦公區。

(四) 未經授權不得將設備、軟體、儲存資訊之媒體或機敏文件攜出電腦機房或辦公環境。若有需要應經主管人員核准，始得進行。

(五) 資訊設備媒體運送過程，應有妥善的安全措施，以防止資料遭竄改、破壞、誤用或未經授權的取用。

二、其他安全管理

(一) 電腦機房實施門禁安全控管。

(二) 資訊支援或維護服務人員，需由管理人員陪同並經登記後，始得進出管制區域。

(三) 電腦機房及各項軟、硬體設備，應強化設（放）置處之防護措施，避免因水患、風災、火災等災害，造成意外損失。

(四) 列印之各式報表、作業程序目錄、及系統文件等保密資料應納入管理。

(五) 資訊設備媒體儲存的資料，不再繼續使用或逾保存年限時，應將儲存的內容，以實體破壞的方式消除；報廢時，應由專人以安全的方式處理，例如：燒燬、水解、碎紙機處理，若可能，應以實體破壞的方式，達到完全清除效果。

第十條　本規範經行政會議通過，陳請校長核定後公布實施，修正時亦同。