臺北市立弘道國中資訊安全計畫

壹、目的

為推動所屬各單位，強化資訊安全管理，確保本校資料、系統、設備及網路安全，特訂定本計畫。

貳、通則

一、本計畫所稱各單位，指本校所屬各辦公室、行政處室、專科教室。

二、各單位應依有關使用規範，考量日常業務以及使用情況，進行資訊安全風險評估，確定各項資訊作業安全需求水準，採行適當及充足之資訊安全措施，確保各單位資訊蒐集、處理、傳送、儲存及流通之安全。

三、本計畫所稱適當及充足之資訊安全措施，應綜合考量各項資訊資產之重要性及價值， 以及因人為疏失、

蓄意或自然災害等風險，致相關資訊資產遭不當使用、洩漏、竄改、破壞等情事，影響及危害機關業務之程度，採行與資訊資產價值相稱及具成本效益之管理、作業及技術等安全措施。

四、本計畫，特針對下列事項，訂定資訊安全計畫實施，並定期評估實施成效：

(一)資訊安全政策訂定。

(二)資訊安全權責分工。

(三)人員管理及資訊安全教育訓練。

(四)電腦系統安全管理。

(五)網路安全管理。

(六)系統存取控制管理。

(七)系統發展及維護安全管理。

(八)資訊資產安全管理。

(九)實體及環境安全管理。

(十)業務永續運作計畫管理。

(十一)其他資訊安全管理事項。

五、本計畫所稱資訊安全政策，指本校為達成資訊安全目標訂定之資訊安全管理作業規定、措施、標準、規範及行為準則等。

參、資訊安全政策

一、明定有關人員在資訊安全作業應扮演之角色，責任分配，以作為各單位之權責分工依據。

二、加強宣導資訊安全政策及相關作業規定，並辦理資訊安全教育訓練。

三、衡酌業務需求，研訂各項資訊安全作業程序，並以書面、電子或其他方式通知員工及與本部連線作業之相關機關（構）、提供資訊服務之廠商。

四、加強電腦網路系統之安全及品質，確保網路傳輸資料的正確性及效率。

五、明定各項系統及網路服務之使用權限，建立安全控管機制，並防止未經授權的系統存取。

六、在發展應用系統時，應有效防範不當軟體及電腦病毒等危害系統安全之情況發生。

七、建立安全防護措施，避免資訊設施遭誤用或人為破壞，並防止業務目的以外或超出授權範圍之使用。

八、確保資訊業務之正常運作，避免人為或意外因素可能導致的威脅，並建立備援及緊急應變處理機制。

九、維護各項資訊業務之正常運作，嚴禁惡意攻擊或傳送等不當行為。

十、具體安全措施：

(一)本校各網路連外節點，均須透過網路防火牆管控。

(二)網路防火牆策略：

1、本校提供之網路服務含 HTTP、POP3(任何收信主機)、SMTP(僅可由本部 Mail 主機寄信)、FTP 及其它因公務需要而提供之服務。

2、資訊人員得運用網路防火牆等相關設備建立管制機制，防止非公務用途或影響網路安全之網路服務。

3、各單位電腦使用之 IP 均採固定式 IP，由本校資訊組賦予，嚴禁使用者任意更改。

4、各單位未經資訊人員同意，不得增設或移除無線基地台、路由器、防火牆、數據機等對外連線設備，亦不得擅自修改相關設定。

5、嚴禁各單位自行開放本校內部網路與外界網路之連線作業，各單位非經本校權責單位同意不得自行與外界網路相連。

6、定期稽核各單位資訊安全作業，以避免資訊災害發生。

7、各應用系統應紀錄稽核必要資訊，定期提供權責人員進行查核，以避免內部人員不當使用。

8、非本校電腦連接上本校內部網路時，使用者必須防範不當軟體及電腦病毒等危害本校其他電腦之系統安全。

肆、組織及權責

(一)資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由本校資訊組負責辦理。

(二)資料及資訊系統之安全需求研議、管理及保護等事項，由各業務單位負責辦理。

伍、人員管理及資訊安全教育訓練

(一)人員安全管理

1、對資訊相關職務及工作，應進行安全評估，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。

2、各單位對於存取重要性與敏感性資訊或系統操作之人員應依相關法令課予軟硬體保管及資料機密維護責任，並加強工作評估、考核，於人員離（休）職時，並應將重要業務最新備份檔案移交列入機關人員職務異動之必要手續。

(二)教育訓練

1、依教職員工角色及職務層級，進行適當的資訊安全講習(如：資訊安全、病毒介紹及其偵防作業等)，促使教職員工瞭解資訊安全的重要性，各種可能的安全風險，以提高教職員工資訊安全意識，促其遵守資訊安全規定。

2、隨時公告資訊安全相關訊息。

陸、電腦系統安全管理

(一)電腦主機、各應用伺服器等設備應設置於專用機房，並指定專人負責管理。

(二)個人電腦及各項周邊設備等應依業務性質及場地空間等因素做妥適的配置，重要設備並應連接不斷電設備系統之電腦專用插座以確保供電之穩定，以防設備受損。

(三)資源使用、設備維護狀況應做成紀錄，設備故障並應儘速排除或聯繫維護廠商處理。

(四)各單位使用有智慧財產權的軟體，應遵守相關法令及契約規定，非經合法授權及與業務無關之軟體，不得安裝使用，否則除應負有關法律責任外，倘導致各單位設備毀損，並應負相關損害賠償責任。

(五)各單位應定期執行必要的資料及軟體備援作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。儲存媒體應存放於安全之環境，並定期更換以確保資料之完整可用。

(六)資訊業務委外時，應於事前審慎評估可能的潛在安全風險（例如資料或使用者通行碼被破解、系統被破壞或資料損失等風險），並與廠商簽訂適當的資訊安全協定，以及課予相關的安全管理責任，並納入契約條款。

柒、網路安全管理

(一)開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

(二)與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。

(三)應安裝企業版之防毒軟體，建置入侵偵測、弱點分析等防駭軟體以保護機關內部網路免於受病毒感染及惡意軟體或駭客入侵之情事發生，此外設備應隨時上網下載、更新最新病毒碼、主機作業系統漏洞修補等。

(四)網路如發現有被入侵或有疑似被侵入情形，應依資通安全處理小組作業要點等相關規定及處理程序，採取必要的行動。

捌、系統存取控制

(一)使用者新進、調整職務及離（休）職時，應以書面通知人事及各應用系統之作業單位或負責人，各應用系統負責人並應依通知及連線作業使用者申請，新增、調整或刪除其使用權限，確保系統安全。

(二)任何帳號皆必須設定通行密碼，使用者通行密碼應符合安全原則，建議使用最少六位長度的通行密碼並應定期更改通行密碼（建議至少三個月一次為原則，最長不宜超過六個月）。

(三)人員暫時離開時應使用鍵盤鎖或其他控管措施保護電腦設備，不使用電腦設備時，必須完全登出電腦系統或離線。

(四)對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並課其相關安全保密責任。

玖、系統發展及維護安全管理

(一)系統之開發建置、維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、後門及電腦病毒等危害系統安全。

(二)對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期或臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

(三)委託廠商建置及維護重要之軟硬體設施，應在本校相關人員監督及陪同下始得為之。

拾、業務永續運作之規劃

(一)各單位應訂定業務永續運作計畫，評估各種人為及天然災害對機關正常業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

(二)如發生資訊安全事件（包括系統有安全漏洞、遭受非法入侵及破壞、遭遇阻斷服務攻擊及功能不正常事件等），致電腦系統無法運作或影響執行效率時，應迅速通報電腦中心人員及單位主管，本校資安聯絡人並應視情節依行政院國家資通安全會報相關規定向上通報。

(三)各單位應依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及充足之資訊安全措施。

拾壹、其他

各單位應就設備安置、周邊環境及人員進出管制等，訂定妥善之實體及環境安全管理措施。

拾貳、本資訊安全計畫陳　校長核可後實施，修正時亦同。