國立竹南高級中學
存取控制管理守則

一、網路安全控管

（一）本機關之網路區域劃分如下：

1. 外部網路：對外網路區域，連接外部廣網路 (Wide Area Network, WAN)。

2. 非軍事區(DMZ)：放置對外服務伺服器之區段。

3. 內部區域網路 (Local Area Network, LAN) ：內部單位人員及內部伺服器使用之網路區段。

（二）外部網路、非軍事區及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

（三）應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。

（四）對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。

（五）內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

（六）對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

（七）使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

（八）網域名稱系統(DNS)防護

1. 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

2. DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

3. 內部主機位置查詢應指向機關內部 DNS 伺服器。

（九）無線網路防護

1. 機密資料原則不得透過無線網路及設備存取、處理或傳送。

2. 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

3. 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

4. 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

二、 資通系統權限管理

（一）本機關之資通系統應設置通行碼管理，通行碼之要求需滿足：

1. 通行碼長度 8 碼以上。

2. 通行碼複雜度應包含英文大寫小寫、特殊符號或數字其中三種以上。

3. 使用者每 90 天應更換一次通行碼。

（二）使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

（三）使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

三、特權帳號之存取管理

（一)資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

（二）資通系統之特權帳號不得共用。

（三）對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

（四）資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

（五）資通系統管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

四、加密管理

（一）機密資訊於儲存或傳輸時應進行加密。

（二）加密保護措施應遵守下列規定：

1. 應落實使用者更新加密裝置並備份金鑰。

2. 應避免留存解密資訊。

3. 一旦加密資訊具遭破解跡象，應立即更改之。