

# 高英高級工商職業學校資訊安全管理要點

100年3月21日行政會報通過

102年8月29日102學年度第1學期期初校務會議修訂通過

104年8月28日104學年度第1學期期初校務會議修訂通過

壹、目的：依據「行政院及所屬各機關資訊安全管理要點」，為強化本校資訊安全管理，建立安全及可信賴之電子化系統，確保資料、系統、設備及網路之安全，特訂定本要點。

## 貳、組織及權責分工

一、本校有關資訊安全管理事務依下列分工原則：為統籌、協調、研議本校各項資訊安全之政策、計畫及資源調度，特成立「資訊安全管理小組」。

二、「資訊安全管理小組」設置資訊安全長（召集人）由校長兼任；資訊安全總幹事由教務主任兼任；執行秘書為資訊科主任兼任；並由秘書、各處室主任、各科主任、資訊專長人員共同組成（如下表）；各處室主任及各科主任、教學組長為單位稽核人員。

職 務	職 稱
資訊安全長兼召集人	校 長
資訊安全副召集人	教務主任
執行秘書	資訊科主任
委 員	學務主任
委 員	總務主任
委 員	實習主任
委 員	圖書館主任
委 員	輔導主任
委 員	人事主任
委 員	會計主任
委 員	主任教官
委 員	教學組長
委 員	汽車科主任
委 員	電機科主任
委 員	廣設科主任
委 員	資處科主任
委 員	餐管科主任
委 員	美容科主任

三、本小組各成員之任務如下：

### （一）資訊安全長：

1. 由校長擔任本小組之召集人，副召集人協辦統籌資訊安全政策、計畫及技術規範之研議以及擬定或修正本校資訊安全政策。

2. 督導及稽核資訊安全政策執行狀況及成效。

(二) 執行秘書：

1. 協助制定、執行及修正資訊安全政策。
2. 決定單位內資安事件通報及應變處理事宜。
3. 監督通報作業、應變計畫及資安演練之實施。
4. 依據資安事件等級，授權系統復原作業之實施。
5. 負責對內、對外之資訊安全聯繫事宜。
6. 負責鑑定資安事件並依程序進行通報作業。
7. 隨時掌握國家資通安全會報或相關單位提供之資通安全危害通告資訊(如最新電腦病毒疫情、漏洞及駭客攻擊資訊等之預警訊息)。
8. 發布資安訊息給校內所有人員，與系統管理人員保持連繫，並負責通告及監督系統漏洞修補與更新。

(三) 稽核人員

1. 協助單位每年實施內部稽核 1 次。
2. 依據資安檢核表評估單位整體資安風險，提出改善建議事項。
3. 協助資安事件之偵防演練作業。

三、本校每年進行一次資訊安全稽核。由各處室與各科主任先做內部資安稽核(電腦安全自我檢查表，如附件)，發現問題記錄並反應至資訊安全小組協助處理。

參、人員管理及資訊安全教育訓練

- 一、各單位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，並進行必要之考核；各單位對可存取機密性或敏感性資訊或系統之人員，及因工作需要須配賦系統存取特別權限之人員，應加強評估及考核。
- 二、各單位負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，實施人員輪調，建立人力備援制度。
- 三、資訊作業相關人員離職時，應取消其個人帳號和使用權限，並確實做好電腦軟硬體及相關文件之移交工作。
- 四、各單位業務主管應負責督導所屬員工之資訊作業安全，防範不法及不當行為。
- 五、資訊安全教育訓練及宣導事宜由資訊安全小組負責辦理。

肆、電腦系統安全管理

- 一、各單位辦理資訊業務委外作業時，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約中，要求廠商遵守及定期考核，並派員監督。
- 二、電腦系統作業變更時，應詳實建立紀錄，以備查考。
- 三、各單位應依相關法規或契約規定，複製及使用軟體；嚴禁使用非法軟體。
- 四、電腦系統中應裝置防毒軟體並定期更新，磁片或隨身碟使用前應事先做掃毒檢查，以防止感染電腦病毒。
- 五、應遵守智慧財產權相關規定，使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。
- 六、應依據電腦處理個人資料保護法等相關規定，審慎處理個人資訊。

伍、網路安全管理

- 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，機密、敏感性或未經當事人同意之個人隱私資料及文件，不得上網公佈。

- 二、本校非屬機密性或敏感性之資料及文件得以電子郵件或其他電子方式傳送。機密性或敏感性之資料及文件，欲利用電子郵件或其他電子方式傳送時，須以適當的加密或電子簽章等安全技術處理。

#### 陸、系統存取控制

- 一、各單位對電腦資料庫及檔案應建立分級（機密及安全等級）管理制度。
- 二、各項正式作業之電腦系統操作及資料處理，由各權責單位指定專人負責建檔、核對、更新、審查及維護電腦資料之正確性。資訊系統發展人員非經核准不得操作使用或更改已正式作業之系統檔案。
- 三、電腦資料庫及檔案，應按不同業務範圍及使用權限，分別設定目錄、識別保護碼；重要或具機密性資料在建檔或提供使用時，應加設通行密碼、使用權限碼，以確保資料安全，且通行密碼應經常更新。
- 四、各單位離職、休職、調職人員，應立即取消使用單位內各項資源之所有權限和個人帳號，並列入人員離職、休職、調職之必要手續；人員職務調整及調動，應依系統存取授權規定，限期調整其權限。
- 五、各電腦系統應建立系統使用者註冊管理制度，建立使用人員名冊。
- 六、各單位之重要資料及系統委外廠商處理者，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

#### 柒、系統發展及維護安全管理

- 一、各單位自行開發或委外發展之系統，應在系統之初始階段即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動等作業，應予安全管制，避免不當軟體及電腦病毒危害系統安全。
- 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；基於實際作業需要，得核發短期性及臨時性之系統辨識與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軟硬體設施時，應在本校相關人員監督及陪同下始得為之。

#### 捌、資訊資產安全管理

- 一、各單位對於儲存各項機密資料或程式軟體之磁片、磁碟、磁帶、光碟片及報表等媒體，應設專人管理並定期備份，防止資料洩漏或損毀。
- 二、對於需要長期保留或重要檔案之備份資料，應存放在防火、防潮、防磁的設備中。

#### 玖、實體及環境安全管理

- 一、各單位對於電腦設備之裝置地點，應考量使用及管理上之安全，並應指定專人負責管理，非經奉准之人員，不得隨意操作設備。管理或使用人員應詳細記載電腦設備故障、異常及維護等情形，以作為設備更新及作業安全之依據。
- 二、電腦設備機房或電腦教室應設置適當之滅火設備。管理人員下班後，應關閉門窗及不必要之電源，以確保安全。

- 拾、業務永續運作之規劃：若發生資訊安全事件，應立即向相關人員通報，以採取適當反應措施。若有情節嚴重者，則聯繫檢警調單位協助偵查。

- 拾壹、本要點經行政會議通過，呈校長核准後實施，修正時亦同。

## 高英高級工商職業學校 電腦安全自我檢查表

請同仁依續檢查辦公室電腦，並於檢查結果欄位勾選是否完成、簽名，經單位主管核章後，送交教務處彙整

編號	檢查項目	檢查結果	檢查說明	個人電腦資訊安全設定操作步驟
1	已完成電腦系統帳號密碼設定	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 系統重新開機查看是否需要登入帳號 2. 檢查是否輸入密碼，密碼至少為 8 碼，並檢查密碼強度	WindowsXP 密碼設定
2	已完成螢幕保護密碼設定	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 請參考步驟 2. 電腦螢幕桌面按右鍵->選螢幕保護程式->設定 10 分鐘以內->點選「繼續後，以密碼保護」	螢幕保護程式密碼設定
3	已關閉資源分享	<input type="checkbox"/> 是 <input type="checkbox"/> 否	完成以下三個功能，請參考操作步驟： 1. 取消 <input type="checkbox"/> File and Printershering for Microsoft Networks 2. 停用 [NetBIOS over TCP/IP] 3. 停止共用資源	※關閉資源分享設定 ※停止共用資源設定
4	無來路不明或未授權軟體	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 檢查程式/未授權程式： a. 查看控制台->新增/移除程式 b. 查看開始->程式集 ※檢查重點： . 未公告授權使用商用軟體 . 遊戲影音寄件系統輔助等來路不明軟體。 2. 檢查未授權檔案： a. 搜尋:dat, mp3, avi, mpg, ape, rm, rmvb 等副檔名。 b. 檢查重點:查看歌曲, 影片及其他檔案是否合法授權, 3. 如有發現來路不明或未授權檔案, 請立即移除。	檢查新增移除程式
5	已安裝防毒軟體	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 檢查電腦右下角是否有防毒軟體圖示 2. 使用外來檔案，應先掃毒，請勿任意移除或關閉防毒軟體。 3. 是否裝有隨身碟防毒軟體 註:如自行安裝防毒系統應具主機防火牆功能	
6	無遠端桌面遙控軟體	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 檢查電腦右下角是否有遠端桌面遙控軟體圖示 2. 如有發現其他遠端桌面遙控軟體, 請立即移除	檢查新增移除程式
7	已完成瀏覽器安全設定	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 參考操作步驟 2. 瀏覽器安全等級應設定為中級或更高，執行特殊程式如須降低安全性，請通知本中心進行安全檢查及管理。 3. 取消瀏覽器設定:自動完成表單的使用者帳號和密碼	※調整 Internet Explorer 安全性 ※如何將網站加入信任
8	郵件軟體已關閉信件預覽	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 參考操作步驟(以 Outlook Express 及 Outlook 為例)	關閉郵件預覽功能
9	無 eDonkey、BT 等 P2P 軟體	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 查看控制台->新增/移除程式 檢查重點： p2p 軟體例: (eDonkey, eMule, ezPeer, BitTorrent(BT), Kuro, BitComet, WinMX, Kazaa, uTorrent, Azureus(JAVA), BitABC, BitTornado, eXeem, Shareaza) 等名稱。	檢查新增移除程式

10	無 Web、FTP、Mail 等網路設站服務	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 網路檢查: a. 開始->執行->cmd -> 輸入 netstat -abn b. 檢查是否有 listening 80, 25, 21 2. 如有發現 web, ftp, mail 等各種網路服務, 請立即移除	服務埠檢查
11	已完成 MS-Office 軟體巨集安全設定	<input type="checkbox"/> 是 <input type="checkbox"/> 否	檢查 windows office 軟體, 如 word, excel, ppt, frontpage 軟體, 是否完成巨集安全設定	設定 Office 巨集安全性
12	Guest 帳號已關閉	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 參考操作步驟	Guest 帳號關閉設定
13	隔離機密性敏感性檔案資料	<input type="checkbox"/> 是 <input type="checkbox"/> 否	機密性敏感性檔案資料應進行實體隔離, 請勿存放於個人電腦中。	
14	開啟 WINDOWS 系統自動更新程式	<input type="checkbox"/> 是 <input type="checkbox"/> 否	同仁應配合進行軟體更新, 修補漏洞, 保持更新至最新狀態, 勿自行關閉系統自動更新程式。	開啟 WINDOWS 系統自動更新程式
16	無閱覽不當之網站	<input type="checkbox"/> 是 <input type="checkbox"/> 否	禁止於上班時間閱覽不當之網路(如暴力、色情、賭博、駭客、惡意網站、釣魚詐欺、傀儡網路等)及瀏覽非公務用途網站, 以避免內部頻寬壅塞	
18	重要業務文件已備份	<input type="checkbox"/> 是 <input type="checkbox"/> 否	1. 養成定時備份資料之習慣 2. 分每星期、每月、每學期及每學年方式備份於光碟或非本機之硬碟上並分開保管並適當加密。 3. 注意資料敏感性, 勿為他人所利用	

單位：

職稱：

姓名：

單位主管：