

# 臺中市大甲工業高級中等學校

## 資通安全維護計畫

版次：V1.0(初版)

資通安全責任等級	<input type="checkbox"/> A 級 <input type="checkbox"/> B 級 <input type="checkbox"/> C 級 <input checked="" type="checkbox"/> D 級 <input type="checkbox"/> E 級
修訂人核章	
單位主管核章	
資安長核章	

中華民國 108 年 1 月 24 日

# 臺中市大甲工業高級中等學校

## 資通安全維護計畫

### 文件制/修訂紀錄表

文件版本	修訂日期	修訂內容	修訂單位	修訂人	核定人 (資安長)
V1.0(初版)	108 年 1 月 24 日	新擬訂文件	教務處	林世原	徐銘宏

# 臺中市大甲工業高級中等學校

## 資通安全維護計畫

### 目 錄

壹、 依據及目的 .....	1
貳、 適用範圍 .....	1
參、 非核心業務及說明 .....	1
一、 非核心業務及說明： .....	1
肆、 資通安全政策及目標 .....	1
一、 資通安全政策 .....	1
二、 資通安全目標 .....	2
三、 資通安全政策及目標之核定程序 .....	2
四、 資通安全政策及目標之宣導 .....	2
五、 資通安全政策及目標定期檢討程序 .....	2
伍、 資通安全推動組織 .....	2
一、 資通安全長 .....	2
二、 資通安全推動小組 .....	3
陸、 專職(責)人力及經費配置 .....	4
一、 專職(責)人力及資源之配置 .....	4
二、 經費之配置 .....	4
柒、 資通安全防护及控制措施 .....	5
一、 存取控制與加密機制管理 .....	5
二、 作業與通訊安全管理 .....	6
捌、 資通安全事件通報、應變及演練相關機制 .....	8
玖、 資通安全情資之評估及因應 .....	8
一、 資通安全情資之分類評估 .....	9
二、 資通安全情資之因應措施 .....	9
壹拾、 資通安全教育訓練 .....	10
一、 資通安全教育訓練要求 .....	10
二、 資通安全教育訓練辦理方式 .....	10

壹拾壹、 公務機關所屬人員辦理業務涉及資通安全事項之考核機制	10
壹拾貳、 資通安全維護計畫及實施情形之持續精進及績效管理機制	11
一、 資通安全維護計畫之實施.....	11
二、 資通安全維護計畫實施情形之稽核機制.....	11
三、 資通安全維護計畫之持續精進及績效管理.....	11
壹拾參、 資通安全維護計畫實施情形之提出 .....	11

## 壹、依據及目的

本計畫依據資通安全管理法第 10 條及施行細則第 6 條訂定。

## 貳、適用範圍

本計畫適用範圍涵蓋臺中市大甲工業高級中等學校 (以下簡稱本校)。

## 參、非核心業務及說明

### 一、非核心業務及說明：

本校之非核心業務及說明如下表：**(請檢視是否使用下列共通性行政系統，並請依現況調整增減)**

非核心業務	業務失效影響說明	最大可容忍中斷時間
公文電子交換系統	電子公文無法即時送達機關，影響機關行政效率	12 小時
校務行政系統	無法使用校務行政系統，影響機關行政效率	12 小時
郵件服務系統	無法使用 e-mail，影響機關行政效率	12 小時
薪資系統	影響機關行政效率	8 小時/上班日
防火牆系統	有資安風險疑慮	12 小時/上班日
其他-非屬上開業務範疇者	影響機關行政效率	24 小時

## 肆、資通安全政策及目標

### 一、資通安全政策

為使本校業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，特制訂本政策如下，以供全體同仁共同遵循：

1. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本校同仁亦應確實參與訓練。
2. 針對辦理資通安全業務有功人員應進行獎勵。
3. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
4. 禁止多人共用單一資通系統帳號。
5. 不得私接網路。
6. 安裝防毒系統。
7. 電腦建立帳號密碼，並依職責設定使用權限。

## 二、資通安全目標

1. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
2. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 6% 及 5%。

## 三、資通安全政策及目標之核定程序

資通安全政策由本校教務處設備組簽陳資通安全長核定。

## 四、資通安全政策及目標之宣導

1. 本校之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。
2. 本校應每年向利害關係人(例如與機關連線作業有關單位)進行資安政策及目標宣導，並檢視執行成效。

## 五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於內部會議中檢討其適切性。

## 伍、資通安全推動組織

### 一、資通安全長

依本法第 11 條之規定，本校指派教務主任擔任資通安全長，負責督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。

2. 資通安全責任之分配及協調。
3. 資通安全資源分配。
4. 資通安全防護措施之監督。
5. 資通安全事件之檢討及監督。
6. 資通安全相關規章與程序、制度文件核定。
7. 資通安全管理年度工作計畫之核定
8. 資通安全相關工作事項督導及績效管理。
9. 其他資通安全事項之核定。

## 二、資通安全推動小組

### (一) 組織

為推動本校之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各處室成立資通安全推動小組<sup>1</sup>，其任務包括：

1. 跨部門資通安全事項權責分工之協調。
2. 應採用之資通安全技術、方法及程序之協調研議。
3. 整體資通安全措施之協調研議。
4. 資通安全計畫之協調研議。
5. 其他重要資通安全事項之協調研議。

### (二) 分工及職掌

本校之資通安全推動小組依資通安全長之指示負責下列事項，本校資通安全推動小組分組人員名單及職掌應列冊，並適時更新之<sup>2</sup>：

(1) 資通安全政策及目標之研議。

(2) 訂定機關資通安全相關規章與程序、制度文件，並確保相關

---

<sup>1</sup> 資通安全推動小組成員由機關之資通安全長召集組成，依資通安全長之指示，負責協助或與機關內之相關單位合作推動機關內部之資通安全業務，如機關未成立資通安全推動小組，相關業務則應由資通安全長責承相關資通安全權責人員辦理之。

<sup>2</sup> 各公務機關應製作「資通安全推動小組成員及分工表」，說明小組成員及相關職掌。

規章與程序、制度合乎法令及契約之要求。

- (3) 傳達機關資通安全政策與目標。
- (4) 資通安全相關規章與程序、制度之執行。
- (5) 資料及資通系統之安全防護事項之執行。
- (6) 資通安全事件之通報及應變機制之執行。
- (7) 其他資通安全事項之規劃與推動。
- (8) 每年至少召開 1 次會議，提報資通安全事項執行情形。

## 陸、專職(責)人力及經費配置

### 一、專職(責)人力及資源之配置

1. 本校依資通安全責任等級分級辦法之規定，屬資通安全責任等級 D 級，設置一名兼辦資通安全業務負責本校之法遵義務、教育訓練及資通安全事件通報及應變等業務之推動。本校現有資通安全專責人員名單及職掌應列冊，並適時更新<sup>3</sup>。
2. 本校之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本校之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。
3. 本校之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。
4. 專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

### 二、經費之配置

1. 資通安全推動小組於規劃配置相關經費及資源時，應考量本校之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源<sup>4</sup>。
2. 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資

<sup>3</sup> 各公務機關應製作「資通安全專職人員分工表」，說明專職人員及相關職掌，格式可參附件：資通安全推動小組成員及分工表。

<sup>4</sup> 為有效建置機關之資通安全風險防護機制，公務機關應投入相當之資源，故機關之資通安全推動小組於資源規劃或編制預算時，應考量機關之責任等級、資通安全政策及目標。



通安全推動小組提出<sup>5</sup>，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。

3. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

## 柒、資通安全防護及控制措施

本校依據自身資通安全責任等級之應辦事項，採行相關之防護及控制措施如下：

### 一、存取控制與加密機制管理

#### (一) 網路安全控管

1. 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。
2. 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。
3. 本校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。
4. 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。
5. 遵循本校校園網路使用規範。
6. 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) 行動通訊等無線設備原則不得攜入涉及或處理機密資料之區域。
  - (3) 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

1. 本校之資通系統應設置通行碼管理，通行碼之要求需滿足下列原則：

---

<sup>5</sup> 各校可填具資通安全需求申請單，格式可參附件：資通安全需求申請單。

- (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、特殊符號或數字三種以上。
  - (3) 使用者每 180 天應更換一次通行碼。
2. 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。
  3. 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。

## 二、作業與通訊安全管理

### (一) 防範惡意軟體之控制措施

1. 本校之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。
  - (1) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。
  - (2) 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。
  - (3) 確實執行網頁惡意軟體掃描。
2. 使用者未經同意不得私自安裝應用軟體，管理者並應定期針對管理之設備進行軟體清查。
3. 使用者不得私自使用已知或有嫌疑惡意之網站。
4. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

### (二) 電子郵件安全管理

1. 本校人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。
2. 電子郵件系統管理人應定期進行電子郵件帳號清查。
3. 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。
4. 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

5. 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。
6. 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。
7. 使用者應確保電子郵件傳送時之傳遞正確性。
8. 使用者使用電子郵件時，應注意電子簽章之要求事項。
9. 本校應配合臺中市政府電子郵件社交工程演練，並檢討執行情形。

### (三) 確保實體與環境安全措施

#### 1. 辦公室區域之實體與環境安全措施

- (1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
- (2) 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。
- (3) 機密性及敏感性資訊，不使用或下班時應該上鎖。
- (4) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。
- (5) 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。
- (6) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

### (四) 媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
2. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。
4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感

之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

#### (五) 電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過十分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
5. 下班時應關閉電腦及螢幕電源。
6. 如發現資安問題，應主動循機關之通報程序通報。
7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

#### (六) 行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。
2. 機敏會議或場所不得攜帶未經許可之行動設備進入

### 捌、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本校依「臺中市政府暨所屬公務機關資通安全事件通報及應變管理程序」暨「學校資通安全事件通報及應變管理程序」辦理資通安全事件通報、應變及演練<sup>6</sup>。詳見本校所訂之資通安全事件通報及應變程序。

### 玖、資通安全情資之評估及因應

本校接獲資通安全情資，應評估該情資之內容，並視其對本校之影響、本校可接受之風險及本校之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

---

<sup>6</sup> 各校應另訂定資通安全事件通報及應變程序。

## 一、資通安全情資之分類評估

本校接受資通安全情資後，應指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

### (一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

### (二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

### (三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

## 二、資通安全情資之因應措施

本校於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

### (一) 資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

### (二) 入侵攻擊情資

由資通安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

### (三) 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

### (四) 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

## 壹拾、資通安全教育訓練

### 一、資通安全教育訓練要求

本校依資通安全責任等級分級屬 D 級，一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

### 二、資通安全教育訓練辦理方式

1. 每年參加中央機關、臺中市政府辦理之資通安全教育訓練或利用數位學習以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄<sup>7</sup>。
2. 員工報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。
3. 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

## 壹拾壹、公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本校所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、臺中市政府及所屬各機關學校公務人員平時獎懲案件處理要點，及本校各相關規定辦理之。

---

<sup>7</sup> 公務機關辦理教育訓練時，參加人員應簽名留存紀錄，格式可參附件：資通安全認知宣導及教育訓練簽到表。

## 壹拾貳、資通安全維護計畫及實施情形之持續精進及績效管理機制

### 一、資通安全維護計畫之實施

為落實本安全維護計畫，使本校之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本校之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

### 二、資通安全維護計畫實施情形之稽核機制

#### (一) 稽核機制之實施

本校應配合上級或監督機關之規定辦理查核作業，以確認人員是否遵循本計畫與機關之管理程序要求，並有效實作及維持管理制度。

#### (二) 稽核改善報告

受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

### 三、資通安全維護計畫之持續精進及績效管理

1. 本校之資通安全推動小組應每年至少一次召開內部會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
2. 持續改善機制應做成改善績效追蹤報告<sup>8</sup>，相關紀錄並應予保存，以作為審查執行之證據。

## 壹拾參、資通安全維護計畫實施情形之提出

本校依據本法第 12 條之規定，依主管機關規定期限向上級或監督機關，提出資通安全維護計畫實施情形<sup>9</sup>，使其得瞭解本校之年度資通安全計畫實施情形。

---

<sup>8</sup> 格式可參附件：改善績效追蹤報告。

<sup>9</sup> 資通安全維護計畫實施情形之內容，包含上開定期評估、稽核機制、缺失之消除或改正及機關辦理資通安全計畫之相關實施事項，參附件：資通安全維護計畫實施情形。