

資通安全組織					
文件編號	HGSH-ISMS-B-001	機密等級	限閱	版次	1.2

1 目的

確保國立新竹女子高級中學（以下簡稱本校）資通安全責任，落實資通安全政策之推行，並符合資通安全管理法及子法：

- 1.1 為確保本校內部資通安全管理事項之推動，應建立適當管理架構，以審核資通安全政策、分配安全責任，並協調本校各項資通安全措施之實施。
- 1.2 建立與外部資通安全專家之聯繫管道，以利於安全事件處理及專家意見徵詢。

2 適用範圍

本校承辦之資通安全相關業務作業流程。

3 權責

無。

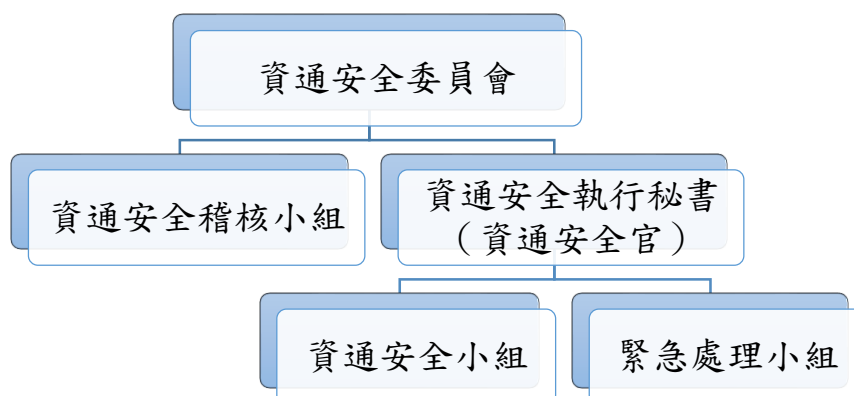
4 名詞定義

無。

5 作業說明

5.1 資通安全組織架構與工作執掌

- 5.1.1 資通安全組織架構如下圖所示，資通安全組織成員應填寫於「資通安全組織成員表」，人員異動亦即時更新。



資通安全組織					
文件編號	HGSH-ISMS-B-001	機密等級	限閱	版次	1.2

5.1.2 資通安全委員會：由本校校長擔任資安長兼召集人，各單位一級主管、各科主任為委員會委員，負責資通安全管理相關事項之決議。

5.1.2.1 每年定期或視需要召開會議，審查資通安全管理相關事宜。

5.1.2.2 視需要召開跨部門之資源協調會議，負責協調資通安全管理執行所需之相關資源分配。

5.1.3 資通安全執行秘書（資通安全官）：由資通安全委員會召集人指派專人擔任。

5.1.3.1 負責協調資通安全小組與緊急處理小組執行資通安全相關作業。

5.1.3.2 負責對資通安全狀況進行預警、監控，並對資通安全狀況與事件進行處置。

5.1.3.3 對於資通安全管理之改善提出建議，以及協助執行資通安全之自我檢核。

5.1.3.4 對於存取控制管理定期進行事件紀錄檢核，以及管理程序檢核。

5.1.4 資通安全小組：由資通安全委員會召集人指派人員組成，負責規劃及執行各項資通安全作業。

5.1.4.1 制定資通安全管理相關規範。

5.1.4.2 推動資通安全相關活動。

5.1.4.3 辦理資通安全相關教育訓練。

5.1.4.4 建立風險管理，執行風險管理。

5.1.4.5 建立安全事件緊急應變暨復原措施。

5.1.4.6 執行稽核改善建議事項。

5.1.4.7 執行預防措施之改善。

5.1.4.8 研討新資通安全產品或技術。

5.1.4.9 執行資通安全委員會決議事項。

資通安全組織					
文件編號	HGSH-ISMS-B-001	機密等級	限閱	版次	1.2

5.1.4.10 鑑別資通安全相關之法規。

5.1.5 緊急處理小組：由資通安全委員會召集人指派人員組成，權責及作業內容分述如下：

5.1.5.1 當重大資安事件發生時，負責通報應變，並聯絡召集緊急處理小組。

5.1.5.2 協調及督導各關鍵業務流程負責人執行作業，並協調資源之調派使用。

5.1.5.3 依據事件評估之結果，得依現況建請資通安全委員會召集人決議是否宣布災變並啟動復原作業。

5.1.5.4 當災變發生時，配合救災單位負責搶救人員、物資與設備等，以及現場指揮工作。

5.1.5.5 負責災後協調、指揮清理災害現場。

5.1.5.6 負責規劃原營運場所之現場復原工作。

5.1.6 資通安全稽核小組：由資通安全委員會召集人指派，負責評估資通安全管理執行情形。

5.1.6.1 擬定資通安全內部稽核計畫。

5.1.6.2 執行資通安全內部稽核。

5.1.6.3 撰寫資通安全內部稽核報告。

5.1.6.4 追蹤不符合事項之改善執行情形。

5.2 管理審查會議

5.2.1 資通安全委員會應每年至少召開一次管理審查會議，必要時得召開臨時會議。

5.2.2 管理審查會議審查內容建議如下：

5.2.2.1 資通安全稽核結果及建議改善事項。

5.2.2.2 上級指導單位、內部同仁及外部單位等利害相關團體的建議。

5.2.2.3 新資通安全產品或技術導入之審查。

資通安全組織					
文件編號	HGSH-ISMS-B-001	機密等級	限閱	版次	1.2

- 5.2.2.4 矯正及預防措施檢討。
- 5.2.2.5 風險評鑑適切性審查。
- 5.2.2.6 前次管理審查會議決議執行狀況。
- 5.2.2.7 影響資通安全管理之任何變更事項。
- 5.2.2.8 資通安全組織成員所提出之改善建議。
- 5.2.2.9 資通安全目標執行狀況報告。

本校依據「資通安全政策」所列之範圍及目標制定「目標值有效性量測表」，並以該量測結果做為評估本校資通安全目標達成情形。

- 5.2.2.10 委外廠商查核暨自我檢核項目表、委外廠商資安管理作業自評表及委外服務案需求規格書之資安條款、資安能力要求項目之適切性。

5.2.3 管理審查會議之結論建議如下：

- 5.2.3.1 資通安全管理執行之各項改進措施。
- 5.2.3.2 更新風險評鑑與風險改善計畫。
- 5.2.3.3 針對可能影響資通安全管理之內、外部事件，修正資通安全管理流程與控制措施，包括：
 - 5.2.3.3.1 營運需求的變更。
 - 5.2.3.3.2 安全需求的變更。
 - 5.2.3.3.3 影響現行營運需求的業務程序變更。
 - 5.2.3.3.4 管理或法規需求的變更。
 - 5.2.3.3.5 契約要求的變更。
 - 5.2.3.3.6 可接受風險等級或標準的變更。
- 5.2.3.4 針對資通安全管理之需要，協調所需之資源。
- 5.2.3.5 控制措施有效性評量方式的改善。
- 5.2.3.6 應每年檢視「目標值有效性量測表」之量測結果與執行情形，並檢討量測項目與目標水準是否需進行調整之必要，做成改善決議。

資通安全組織					
文件編號	HGSH-ISMS-B-001	機密等級	限閱	版次	1.2

6 相關文件

6.1 資通安全政策

6.2 資通安全組織成員表

6.3 目標值有效性量測表

目標值有效性量測表

量測項目	目標值	量測方式	量測結果	說明
社交工程郵件開啟率	≤10%	每年社交工程郵件演練 開啟比率	☐ 符合 ☐ 不符合，_____	
社交工程郵件點閱率	≤6%	每年社交工程郵件演練 點閱比率	☐ 符合 ☐ 不符合，_____	
社交工程郵件附件開啟率	≤2%	每年社交工程郵件演練 附件開啟比率	☐ 符合 ☐ 不符合，_____	
資通安全教育訓練完成率	≥90%	每人每年完成教育訓練 時數	☐ 符合 ☐ 不符合，_____	如：人員教育 訓練實際狀況
備份資料回復測試	1次/年	針對非核心且對外服務 之資通系統，每年辦理 一次備份資料回復測試 紀錄		如：備份資料 回復測試紀錄