國立新竹女子高級中學

資訊安全政策

機密等級：一般

文件編號：HGSH-ISMS-A-001

版 次：1.0

發行日期：108.10.29

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	108.10.29	All	陳肇斐	初版

國立新竹女子高級中學

資訊安全政策					
文件編號	HGSH-ISMS-A-001	機密等級	一般	版次	1.0

目錄

1 目的 1

2 依據 1

3 適用範圍 1

4 目標 2

5 責任 2

6 審查 3

7 實施 3

8 相關文件 3

國立新竹女子高級中學

資訊安全政策					
文件編號	HGSH-ISMS-A-001	機密等級	一般	版次	1.0

1 目的

為確保國立新竹女子高級中學（以下簡稱本校）所屬之資訊資產的機密性、完整性與可用性，導入資訊安全管理系統，強化本校資訊安全管理，保護資訊資產免於遭受內、外部蓄意或意外之威脅，維護資料、系統、設備及網路之安全，提供可靠之資訊服務，訂定本政策。

2 依據

1.1 個人資料保護法（及施行細則）

1.2 行政院及所屬各機關資訊安全管理要點

1.3 教育體系資通安全管理規範

3 適用範圍

3.1 本政策適用範圍為本校之全體人員、委外服務廠商與訪客等。

3.2 資訊安全管理範疇涵蓋 12 項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校造成各種可能之風險及危害，各領域分述如下：

3.2.1 資訊安全政策訂定與評估。

3.2.2 資訊安全組織。

3.2.3 資訊資產分類與管制。

3.2.4 人員安全管理與教育訓練。

3.2.5 實體與環境安全。

3.2.6 通訊與作業安全管理。

3.2.7 存取控制安全。

3.2.8 系統開發與維護之安全。

3.2.9 資訊安全事件之反應及處理。

3.2.10 業務永續運作管理。

3.2.11 相關法規與施行單位政策之符合性。

3.2.12 個人資料保護。

4 目標

維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由本校全體同仁共同努力來達成下列目標：

4.1 保護本校業務服務之安全，確保資訊需經授權，人員才可存取，以確保其機密性。核心業務系統遭非法存取之事件，每年發生次數不得超過 1 次。

4.2 保護本校業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。核心業務系統資料異動經查核異常案件應為 1 件。

4.3 建立本校業務永續運作計畫，以確保本校業務服務之持續運作。提供核心業務系統之平台因資安事件導致服務停頓，每次不得超過 8 小時，每年中斷服務率不得超過 2% 以上（計算方式：全年中斷服務之總工作小時／一年總工作小時）。

4.4 網路服務服務品質，需達全年上班時間網路正常服務時間可用性 98%。

註：計算公式($可用性=1-\frac{中斷時數}{8小時\times5天\times52週}$)

4.5 資料遭未經授權之異動、毀損、誤植或其他非預期性事件影響資料正確性，已衝擊業務正常運作之資安事件，全年不得超過三件。

4.6 校譽傷害、經濟損失、個人權益嚴重受損或犯罪觸法之資安事件，全年不得超過三件。

4.7 每年依本校全體人員之工作職務、責任，適當授與資訊安全相關訓練。

4.8 確保本校各項業務服務之執行須符合相關法令或法規之要求。

5 責任

5.1 本校應成立資訊安全組織統籌資訊安全事項推動。

5.2 管理階層應積極參與及支持資訊安全管理制度，並授權資訊安全組織透過適當的標準和程序以實施本政策。

5.3 本校全體人員、委外服務廠商與訪客等皆應遵守相關安全管理程序以維護本政策。

5.4 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全

事件或弱點。

5.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

6 審查

6.1 本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，並確保本校業務永續運作之能力。

6.2 依據「ISMS 有效性量測表」，定期審查資訊安全管理制度之有效性。

7 實施

本政策經「資訊安全委員會」核定後實施。

8 相關文件

8.1 有效性量測表