國立基隆女子高級中學

資通安全政策

機密等級：一般

文件編號：KLGSH-A-001

版 次：2.0

發行日期：109.09.01

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	109.09.01		圖書館	初版
2.0	112.06.05		圖書館	因應時代變遷變更資安政策之依據為IOS 27001:2022並簡化資安政策之目標。

資通安全政策					
文件編號	KLGSH-A-001	機密等級	一般	版次	2.0

目　錄

資通安全政策					
文件編號	KLGSH-A-001	機密等級	一般	版次	2.0

1 目的

為確保國立基隆女子高級中學（以下簡稱本校）所屬之資訊資產的機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本校之業務需求，訂定資通安全政策(以下簡稱本政策)。

2 依據

2.1 資通安全管理法及其相關子法。
2.2 ISO/IEC 27001:2022 資訊安全-網路安全與隱私保護(Information security, cybersecurity and privacy protection)。

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 本校 ISMS 資訊安全管理制度(Information Security Management System,簡稱 ISMS)所涵蓋範圍內皆適用，而其控制類別分為 4 大類：
3.2.1 資訊安全政策。
3.2.2 人員控制。
3.2.3 實體控制。
3.2.4 技術控制。

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。期藉由本校全體同仁共同努力來達成下列目標：

4.1 確保本校業務相關資訊之機密性，保障本校機密與個人資料。

4.2 確保本校業務相關資訊之完整性及可用性，提高本校行政效能與品質。

4.3 本校業務活動執行須符合相關法令，達成業務持續運作之目標。

4.4 配合國家及本政策之推動，提昇資通安全防護能力。

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. 管理指標

為評量本政策管理目標達成情形，本校特訂定管理指標如下：

6.1 定量化指標

6.1.1 因人為或作業疏失及未經授權的存取之資安事故，每年不得超過2件。

6.1.2 確保本校機房維運服務達全年上班時間98%(含)以上之可用性。

6.1.3 確保滿足各關鍵業務系統之服務可用率達全年上班時間之98%(含)以上。

6.1.4 為確保本校資訊安全措施或規範符合現行法令、法規之要求，每年至少需執行內部稽核1次。

6.1.5 應適當保護本校資訊資產之機密性與完整性，每年至少需進行資訊資產盤點及風險評鑑作業1次。

6.1.6 為確保本校資訊業務服務得以持續運作，每年至少需執行業務永續運作計畫演練1次。

6.2 定性化指標

6.2.1 定期審查本校資訊安全組織人員執掌，以確保資訊安全工作之推展。

6.2.2 應符合主管機關之要求，依員工職務及責任提供適當之資訊安全相關訓練。

6.2.3 應加強本校資訊機房設施之環境安全，採取適當之保護及權限控管機制。

6.2.4 應加強存取控制，防止未經授權之不當存取，以確保本校資訊資產受適當的保護。

6.2.5 確保資訊不會在傳遞過程中，或因無意間的行為透露給未經授權的第三者。

6.2.6 確保所有資訊安全意外事故或可疑之安全弱點，都應依循適當之通報機制向上反應，並予以適當調查及處理。

7 審查

本政策應每年至少審查 1 次，以反映政府法令、技術及業務等最新發展現況，以確保本政策之運作。

8 實施

本政策配合管理審查會議進行審核，經管理審查會議核定後實施，修訂時亦同。