國立花蓮高級工業職業學校

資通安全政策

機密等級：一般

文件編號：**HLIS-A-001**

版 次：**5.1**

發行日期：**112.3.20**

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	108.02.13		汪冠宏	初版
2.0	109.05.01	P1-P2	王巧雲	二、依據 三、資通安全目標
3.0	110.10.05	P2	王巧雲	六、資通安全政策及目標需定期檢討審查
4.0	111.10.26	P2	王俊和	三、資通安全目標
5.0	112.3.20	P2	王俊和	三、資通安全目標
5.1	114.5.21	P3	王俊和	三、資通安全目標
5.2	114.12.22	P2	王俊和	三、資通安全目標

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. 建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 應強固核心資通系統之韌性，確保機關業務持續營運。
4. 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。
5. 針對辦理資通安全業務有功人員應進行獎勵。
6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件，加強認識社交工程釣魚郵件對資安危害的宣導。
7. 要求並提醒定期更換個人系統密碼，以維護帳號安全。
8. 禁止多人共用單一資通系統帳號，推廣無線網路個人帳號認證系統的使用。

二、依據

1. 資通安全法(及施行細則)
2. 個人資料保護法（及施行細則）
3. 行政院及所屬各機關資訊安全管理要點

4. 教育體系資通安全暨個人資料管理規範

三、資通安全目標

1. 量化型目標

A.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。

B.確保資訊資產受適當之保護，每年未經授權或因作業疏失對資產所造成的損害 0 件。

C.確保所有資通安全事件或可疑之安全弱點，每年不依適當通報程序反應，並予以適當的調查及處理 0 件。

D.資通系統可用性達 99.9%以上

2. 質化型目標：

A.適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

B.達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。

C.提升人員資安防護意識、防止發生中毒或入侵事件。

D.強化委外廠商之選任、監督、管理，嚴格審視委外契約，建構安全服務通道，確保供應鏈關係之資通安全。

四、資通安全政策及目標之核定程序

資通安全政策由本校設備組簽陳資通安全管理代表核定。

五、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(如校內人員、與機關連線作業有關核心業務單位、及 IT 服務供應商)進行資安政策及目標宣導，並檢視執行成效。

六、資通安全政策及目標定期檢討審查

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及關注方之關注議題，以確保本校資訊安全管理制度之運作。

七、實施

本政策經「資通安全委員會」核定後實施，修訂時亦同。

資安長: