國立苗栗特殊教育學校

資通安全政策

機密等級：一般

文件編號：MLSES-A-001

版　　次：2.0

發行日期：109.10.16

修　訂　紀　錄		
版次	**修訂日期**	**修訂內容摘要**
1.0	109.10.16.	初版
2.0	114.03.19.	增列說明暨資通安全教育訓練事項

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

目　錄

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

1 目的

為確保國立苗栗特殊教育學校（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，特訂定本政策。

2 依據

2.1 個人資料保護法及個人資料保護法施行細則。

2.2 行政院及所屬各機關資訊安全管理要點。

2.3 教育體系資通安全暨個人資料管理規範。

2.4 資通安全法及資通安全法施行細則暨相關辦法。

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 13 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：本政策及依據本政策所訂定之各項附屬規定，係依據資通安全管理法及施行細則等法規及其他相關標準所訂定，資訊使用者應確實遵守，如有違反者，依相關法令辦理。

3.2.2 資訊安全組織：為落實本校資通安全管理，由本校校長擔任資通安

全長，並成立資通安全委員會、資通安全稽核小組、資通安全工作小組及緊急處理組，負責統籌資通安全管理制度相關事項制定、資通安全稽核評估執行情形等事宜，其組織運作及工作職責另定管理程序。

3.2.3 人力資源安全：為降低內部人為因素對本校資通安全之影響，各單位應考量人力及工作職掌，實行分工措施。本校應視需要實施資通安全教育訓練及宣導，以提高人員對資通安全之認知。

3.2.4 資產管理：為保護本校資訊資產安全，應建立資訊資產清冊加以分類分級，並訂定相對應之管制措施。

3.2.5 存取控制：為避免本校資訊資產因未授權之存取而使機密性或敏感性資料遭不當使用，應考量人員職務授予相關權限訂定存取控制管理原則。

3.2.6 密碼學(加密控制)：本校憑證申請及應用原則，應定期進行評估，以保護資訊的機密性、鑑別性及完整性，必要時得採行加解密及身分鑑別機制，以加強資料之安全。

3.2.7 實體及環境安全：為確保本校電腦機房維運及資訊資產使用區域之安全暨行動裝置及可攜式儲存媒體的使用安全，應訂定實體安全管理原則。

3.2.8 運作安全：為確保本校主機作業平台、資料庫與資通處理設施被正

確及安全操作，受到防範惡意碼的保護、防護資料損失及竄改、紀錄事件及產生相關證據、保護作業系統的完整並防止技術脆弱性被利用，應訂定運作與通訊管理作業原則。

3.2.9 通訊安全：為確保本校網路及其支援資通處理設施上資訊之保護，並維護內部及外部單位資訊傳送之安全，應訂定通信與作業管理原則。

3.2.10 系統獲取、開發及維護：為確保本校資通系統生命週期的資通安全控管，分析、設計、開發、測試、上線及維護各階段之資通安全，應訂定系統開發與維護安全管理標準作業原則。

3.2.11 供應者關係：為提高本校委外作業之安全，應要求廠商簽署保密切結書，並管理專案人員及駐點人員之各項資訊資產存取權限。

3.2.12 資訊安全事故管理：為確保本校資通安全事件管理（包括對安全事件及弱點之通報）有一致及有效的作法，應建立資通安全事件通報及應變程序，並加以紀錄。

3.2.13 營運持續管理之資訊安全層面：為避免本校資訊資產遭受災害而影響業務永續運作，確保資訊處理設施的可用性，資通安全持續性應做為營運持續管理之基礎，定期測試演練營運持續緊急應變演練及復原。

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。

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。

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。

4.4 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，本校資安人員每年至少接受 12 小時以上之資安專業課程訓練或資安職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練；資訊人員（即各系統承辦人員）每人每二年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練；一般使用者與主管，每人每年接受 3 小時以上之資通安全通識教育訓練。

4.5 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 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。

5.2 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。

5.3 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。

5.4 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。