國立臺南高級商業職業學校

資訊安全政策

機密等級：一般

文件編號：TNCVS-ISMS-A-001

版 次：1.3

發行日期：113.08.16

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	100.05.24		文管人員	初版
1.1	108.10.29	p.1	文管人員	「1.1電腦個人資料保護法(及施行細則)，修正為「1.1個人資料保護法(及施行細則)」，1.4個人資料保護法刪除。
1.2	111.05.11	p.2	文管人員	「不得超過8小時」 修改為「不得超過24小時」
1.3	113.08.16	p.2	文管人員	修訂資訊安全目標內容。

資訊安全政策					
文件編號	TNCVS-ISMS-A-001	機密等級	一般	版次	1.1

目　錄

資訊安全政策					
文件編號	TNCVS-ISMS-A-001	機密等級	一般	版次	1.1

1 目的

為確保國立臺南高級商業職業學校（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，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 量化型目標

4.1.1 核心資通系統可用性達 99.99%以上。(中斷時數/總運作時數≤ 0.1%)

4.1.2 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。

4.1.3 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5%及 2%。

4.2 質化型目標

4.2.1 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。

4.2.2 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。

4.2.3 即時公告資通安全相關新知，以提升人員資安防護意識。

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

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。

7 實施

本政策經「資訊安全委員會」核定後實施。