國立羅東高級商業職業學校

資訊安全政策

機密等級：一般

文件編號：LTCVS-ISMS- A-001

版　　次：1.1

發行日期：114.03.25

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	110.03.08		許志瑋	初版 110.03.22 資通安全委員會通過
1.1	113.03.12		吳政哲	113.03.12 資通安全委員會通過

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

1 目的

為確保國立羅東高級商業職業學校（以下簡稱本校）所屬之資訊資產的機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，並衡酌本校之業務需求，訂定本政策。

2 適用範圍

資訊安全管理涵蓋 14 項管理事項,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，對本校帶來各種可能之風險及危害。管理事項如下：

2.1 資訊安全政策(訂定與評估)。

2.2 資訊安全組織。

2.3 人力資源安全。

2.4 資產管理。

2.5 存取控制。

2.6 密碼學(加密控制)。

2.7 實體與環境安全。

2.8 運作安全。

2.9 通訊安全。

2.10 資訊系統取得、開發及維護。

2.11 供應者關係。

2.12 資訊安全事故管理。

2.13 營運持續管理之資訊安全層面。

2.14 遵循性。

本校之內部人員、委外服務廠商與訪客皆應遵守本政策。

3 目標

為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之安全，期藉由本校全體同仁共同努力來達成下列目標：

3.1 保護本校核心系統業務活動資訊,避免未經授權的存取,確保其機密性。

3.2 保護本校核心系統業務活動資訊，避免未經授權的修改，確保其正確性與完整性。

3.3 建立資訊業務永續運作計畫，確保本校核心系統業務活動之持續運作。

3.4 本校核心系統之業務活動執行須符合相關法令或法規之要求。

4 責任

4.1 本校應成立資訊安全組織統籌資訊安全事項推動。

4.2 管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序以實施本政策。

4.3 所有人員和委外服務廠商均須依照相關安全管理程序以維護資訊安全政策。

4.4 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。

4.5 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。

5 管理指標

為評量資訊安全管理目標達成情形，本校特訂定資訊安全管理指標如下：

5.1 定量化指標

5.1.1 因人為或作業疏失及未經授權的存取之資安事故，每年不得超過二件。

5.1.2 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。

5.1.3 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。

5.1.4 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 2 年至少需執行內部稽核乙次。

5.1.5 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乙次。

5.1.6 為確保本校資訊業務服務得以持續運作，每 2 年至少需執行業務永續運作計畫演練乙次。

5.2 定性化指標

5.2.1 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。

5.2.2 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。

5.2.3 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。

5.2.4 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。

5.2.5 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。

5.2.6 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。

6 審查

本政策應至少每年審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本校永續運作及提供學術網路服務之能力。

7 實施

7.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

7.2 本政策經「資訊安全委員會」核定後實施。