

國立東華大學 圖書資訊處
(花蓮區域網路中心)

資訊安全政策

機密等級：一般

文件編號：RNC-HDRC-A-001

版 次：V2.1

發行日期：107 年 08 月 01 日

資訊安全政策

文件編號	RNC-HDRC-A-001	機密等級	一般	版次	V2.1
------	----------------	------	----	----	------

目錄

1 目的 1

2 適用範圍 1

3 目標 1

4 責任 3

5 審查 3

6 實施 3

資訊安全政策					
文件編號	RNC-HDRC-A-001	機密等級	一般	版次	V2.1

1 目的

確保國立東華大學圖書資訊處—花蓮區域網路中心（以下簡稱本單位）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。

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，對本單位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。
- 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。

本單位之內部人員、委外服務廠商與訪客皆應遵守本政策。

3 目標

資訊安全政策					
文件編號	RNC-HDRC-A-001	機密等級	一般	版次	V2.1

維護本單位資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。

藉由全體同仁共同努力來達成下列目標：

- 3.1 保護本單位 TANet 與大學學籍核心系統與成績管理系統業務活動資訊，避免未經授權的存取。
- 3.2 保護本單位 TANet 與大學學籍核心系統與成績管理系統業務活動資訊，避免未經授權的修改，確保其正確完整。
- 3.3 建立資訊業務永續運作計畫，確保本單位 TANet 與大學學籍核心系統與成績管理系統業務活動之持續運作。
- 3.4 本單位之業務活動執行須符合相關法令或法規之要求。
- 3.5 透由利害關係者及與議題等要求事項，達成下列目標：
 - 3.5.1 全景與範圍對應其重要業務流程之要求與維運持續。
 - 3.5.2 達成與資安政策一致之預期。
 - 3.5.3 透過可量測的規範進行風險管理過程。
 - 3.5.4 本校之業務活動執行須符合相關法令或法規之要求。
- 3.6 組織欲達成目標需決定相關要點：
 - 3.6.1 執行事項。
 - 3.6.2 所需資源。
 - 3.6.3 負責人員。
 - 3.6.4 完成時間。

資訊安全政策					
文件編號	RNC-HDRC-A-001	機密等級	一般	版次	V2.1

3.6.5 成果評估方式。

3.6.6 各項量測指標(資安工作目標與計畫)、所需資源、負責人員、達成時間及成果評估方式等資訊，請詳閱「ISMS 有效性量測」。

4 責任

4.1 設置本校「資通安全暨個人資料保護宣導及執行小組」，負責政策之督導；另設置本單位「資訊安全委員會」，負責政策之擬定、執行、監督、稽核、資訊安全預防及危機處理。

4.2 資訊安全管理者透過適當的標準和程序以實施此政策。

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單位之相關規定進行議處。

5 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，以確保本單位永續運作及提供學術網路服務之能力。

6 實施

6.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

6.2 本政策經「資訊安全委員會」核定後實施，修訂時亦同。