

等 別：高考二級
類 科：資訊處理
科 目：資訊管理與資通安全研究
考試時間：2 小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

(三)請以黑色鋼筆或原子筆在申論試卷上作答。

(四)本科目除專門名詞或數理公式外，應使用本國文字作答。

一、1986 年 R.O. Mason 提出 PAPA 模式，被廣為採納做為資訊倫理議題的重要框架。請詳述 PAPA 模式的具體內容。(25 分)

二、請詳述企業組織之資訊委外（Outsourcing）的決策因素，並從經濟面、管理面、技術面及策略面分別說明資訊委外的利益。(25 分)

三、隨著美國國家標準及技術研究所（National Institute of Standards and Technology, 簡稱 NIST）逐步公布後量子密碼演算法（Post Quantum Cryptography, 簡稱 PQC）標準，全球各界正加速建立後量子密碼遷移指引（PQC Migration Guideline）。請詳述後量子密碼遷移指引應涵蓋的具體內容。(25 分)

四、使用者身分識別（User Identification）及設備鑑別（Device Authentication）是建立零信任架構（Zero Trust Architecture）的重要基礎。

(一)請說明至少 3 種使用者身分識別方法。(15 分)

(二)請說明至少 2 種設備鑑別方法。(10 分)