代號：50870
頁次：1－1

112年公務人員特種考試警察人員、一般警察人員、國家安全局國家安全情報人員考試及112年特種考試交通事業鐵路人員、退除役軍人轉任公務人員考試試題

考 試 別：警察人員考試
等　　別：三等考試
類科組別：警察資訊管理人員
科　　目：數位鑑識執法
考試時間：2 小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡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。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、請以國內學者所提出數位證據鑑識標準程序（Digital Evidence Forensics Standard Operating Procedure, DEFSOP）四大階段（原理概念階段、準備階段、操作階段、報告階段）為基礎及參考國際資安鑑識相關標準（如 ISO/IEC 27037/27041/27042/27043 等），如何建立一套完整行動鑑識標準作業程序（DEFSOP for Mobile Forensics, DEFSOP-MF）？並請舉例及繪圖表說明之。（25 分）

二、請說明電腦鑑識（Computer Forensics）、軟體鑑識（Software Forensics）、資料鑑識（Data Forensics）、網路鑑識（Network Forensics）、行動鑑識（Mobile Forensics）、雲端鑑識（Cloud Forensics）及資安鑑識（Cyber Forensics）的異同處（含定義、原理、功能及應用等）。並請舉例及繪圖表說明之。（25 分）

三、近年來全球發生勒索病毒（Ransomware）攻擊事件層出不窮，對各行各業的政府部門及企業組織（營運持續性）攻擊犯罪問題帶來了重大威脅。請問透過資安鑑識及系統性的資安風險管理，並結合 NIST Cybersecurity Framework（如 ISO 27110：2021）的 IPDRR 五大功能應用（識別（Identify）、保護（Protect）、偵測（Detect）、應變（Respond）、復原（Recover）），如何有效地降低勒索病毒及其他資安事件對企業營運的影響，並有能力偵辦該網路犯罪事件，進行事前相關的風險評估、防護措施建立、事中應變策略制定，以及事後的修復與檢討，以提高其營運的持續性與恢復力？並請舉例及繪圖表說明之。（25 分）

四、臺灣近年爆發多起重大個資外洩事件，且是從公部門到民間企業私部門，甚至在海外遭販賣；另根據內政部警政署統計，2022-2023 年（網路）詐欺案，也創下 10 年新高紀錄，專家學者指出，很大一部分是來自於個資外洩事故。請從資安鑑識角色（含事前預警系統+事中反應系統+事後復原系統等），說明如何有效偵查及防制上述個資外洩犯罪事故，並提高其數位證據能力及符合資安鑑識基本原則（CIAC Principles）？請用相關國際資安鑑識標準（如 DEFSOP/ISO 27042/27050 等），並請舉例及繪圖表說明之。（25 分）（CIAC Principle 是指 Consistent, Integrity, Accuracy and Compliance）（ISO/IEC 27050:2018-2021 — Information Technology — Security Techniques — Electronic Discovery）