代號：20870
頁次：1－1

115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及移民行政人員考試試題

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、數位證據具有易修改性、無限複製性及原始作者不易確定等特性。請論述並舉例說明「資安鑑識 CIAC 基本原則（適法性、完整性、準確性、一致性）」之具體內涵？（15 分）並解釋鑑識人員在處理行動裝置時，應如何落實「不變更數位證據原則」以確保其法律效力？（10 分）

二、國際標準 ISO/IEC 27050 系列（Information Technology—Electronic Discovery）係針對「電子發現（Electronic Discovery, eDiscovery）」所制定的標準。請說明該標準如何定義「電子儲存資訊（Electronically Stored Information）」的生命週期？（15 分）並請詳述其中「保存（Preservation）」階段如何透過「法律保留通知（Legal Hold）」防止證據遭到惡意破壞？（10 分）

三、依據「打詐 2.0」之後端快速反應機制，在面對詐騙廣告刊登不逾 2 日的高度時效性下，請從電腦犯罪現場偵查角度，論述應如何執行主動式防禦並優先保全揮發性證據（Volatile Evidence）？（10 分）其與 ISO 27035 系列資訊安全事件管理（Information Security Incident Management）國際標準的管理流程之關聯為何？（15 分）

四、結合 ISO/IEC 27043 資安事件調查原則與流程與 ISO/IEC 27037 數位證據識別、收集、獲取與保存指南，請從數位鑑識執法角度，論述數位證據處理程序中的「監管鏈（Chain of Custody）」應如何落實？（15 分）在調查勒索軟體攻擊事件時，如何透過雜湊值（Hash）比對與日誌記錄，確保從「初始化」到「報告」階段的證物不被二次污染？（10 分）