《資通安全》

一、因應政府開放資料（Open Data）的使用及符合相關的個人資料保護規範，請詳述政府機關遂行個人資料去識別化（De-identification）過程應有的具體作為。（25 分）

答題關鍵	本題結合政府法規和個資隱私保護，答題時可從識別個資及風險管理架構寫出去識別化的應有或既有作為，即使對個資保護法或政府政策不熟，也能取得部份分數。

【擬答】

(一)個人資料去識別化之必要性

政府開放資料(Open Data）可增進政府施政透明度、提升民眾生活品質，滿足產業界需求，對於各級政府間或各部會間之決策品質均有助益，可見其重要性，因考量到民眾的應用面、使用端之需求，故開放食、醫、住、行、育樂、就業、文化、經濟發展和生活品質等各部整理之資料集，允許任何人都可以自由存取、使用、修改，以及分享，且最多僅受限於引註出處。

惟政府開放的資料中若涉及個人資料(Personally Identifiable Information, PII)，將有侵害個人隱私權之疑慮。根據個人資料保護法第 28 條規定，公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任，被害人雖非財產上之損害，亦得請求賠償相當之金額，每人每一事件新臺幣五百元以上二萬元以下計算，合計最高總額以新臺幣二億元為限。故應將個人資料去識別化（De-identification）。

依據個人資料保護法與法務部民國 103 年 11 月 7 日法律字第 10303513040 號函釋見解，「去識別化」成為降低侵害的解決方案之一，目前我國已確立有國家標準作為去識別化之驗證標準規範。分別於 103 年 6 月以及 104 年 6 月，CNS29100「資訊技術-安全技術-隱私權框架」、以及 CNS29191「資訊技術-安全技術-部分匿名及部份去連結鑒別之要求事項」，作為現階段個人資料去識別化之驗證標準，並據此制訂「個人資料去識別化過程驗證要求及控制措施」，提供個資去識別化之隱私框架，以下簡要說明控制措施五大章節：

1. 隱私權政策：涉及 PII 處理之組織的高階管理階層，應依營運要求及相關法律與法規，建立隱私權政策，提供隱私權保護之管理指導方針及支持。對應個資法施行細則第 12 條第 2 項第 5 款適當安全維護措施事項「個人資料蒐集、處理及利用之內部管理程序」，即為涉及個資生命週期為保護基礎之管理程序，從蒐集、處理到利用為原則性規範，以建構個資去識別化過程管理系統。
2. PII 隱私風險管理過程：組織應定期執行廣泛之 PII 風險管理活動並發展與其隱私保護有關的風險剖繪。直接對應規範即為個資法施行細則第 12 條第 2 項第 3 款「個人資料之風險評估及管理機制」。
3. PII 之隱私權原則：組織蒐集、處理、利用 PII 應符合之 11 項原則，包含「同意及選擇原則」、「目的適法性及規定原則」、「蒐集限制原則」、「資料極小化原則」、「利用、保留及揭露限制」、「準確性及品質原則」、「公開、透通性及告知原則」、「個人參與及存取原則」、「可歸責性原則」、「資訊安全原則」，以及「隱私遵循原則」。以上原則涵蓋個資法施行細則第 12 條第 2 項之 11 款事項。
4. PII 去識別化過程：組織應建立有效且周延之 PII 去識別化過程的治理結構、標準作業程序、非預期揭露備妥災難復原計畫，且組織之高階管理階層應監督及審查 PII 去識別化過程之治理的安排。個資法施行細則第 17 條所謂「無從識別特定當事人」定義，係指個資以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者，組織於進行去識別化處理時，應依需求、風險評估等確認注意去識別化程度。
5. 重新識別 PII 之要求：此章節為選驗項目，需具體依據組織去識別化需求，是否需要重新識別而決定是否適用；若選擇適用，則保留重新識別可能性，應回歸個資法規定保護個資。

(二)個人資料去識別化之具體作為

1. PII 隱私風險管理(隱私保全考量)
   (1)瞭解組織、技術環境所影響隱私風險之因素 (法規因素、契約因素、營運因素)
   (2)識別及評估組織所擁有 PII 之風險
   (3)需通知 PII 當事人其風險，與之協調以求共識(PII 當事人有權行使對於個人資料增、刪、改、查之權利)
2. PII 去識別化
   (1)以密碼學加密機制或特定規則編碼進行假名化(或稱匿名化)，以達成去識別化之目的。

(2)以 K-匿名法(將確切值隱藏在一個區間達到匿名效果。直覺、容易使用的作法，建議 K 值大於 20，較不易遭攻破)為開放資料之限制條件。

3.PII 去識別化過程要求

(1)組織應對 PII 遭非預期揭露備妥災難復原計畫，應及時回應認為個人資料遭揭露民眾之申述及查詢，並協助其採取必要之彌補措施。

(2)應提供獨立及隔離系統環境進行 PII 去識別化工作，並管制及記錄人員與資料之進出(及存取)，且人員不得攜帶任何具照像及記錄功能之設備進入工作區域。

(3)資料去識別化過程應留下紀錄、全程受監督(例：全程錄影)，且其紀錄應無法竄改，並定期稽核。

(4)委外處理 PII 去識別化時，組織應監督及監視委外處理活動。原始資料以不攜出組織場域為原則。含有 PII 之資料應經組織之高階管理階層核准方可攜出場域外，而受委託單位須依組織之隱私權政策及隱私權原則妥善並安全保存原始資料，並於完成 PII 去識別化後，立即歸還組織或安全銷毀。

(5)應對已移除 PII 之資料進行「重新識別測試」，包含：

A.搜尋網頁，嘗試連結 PII 當事人。

B.搜尋全國或地方新聞資料庫，嘗試連結 PII 當事人。

C.搜尋政府單位或其他組織之開放資料，嘗試連結 PII 當事人。

D.以社群網路嘗試連結 PII 當事人。

二、電子支付（Electronic Payment）是指電子交易的當事人，包括消費者、廠商及金融機構，透過資通訊網路系統或平台進行貨幣支付或資金流轉。請詳述金融機構遂行電子支付業務時必須考量的可能資安風險及因應對策。（25 分）

答題關鍵	作答時應考量電子支付的整個生命週期以及相關之基礎建設所涵蓋的範圍，可假想自己是內部或外部攻擊者，再反向思考該用何種方式進行識別電子支付資安風險，並說明可能之因應對策。

【擬答】

(一)資料安全：在電子支付生命週期中，資料的傳輸、處理及儲存過程皆有外洩或竄改等風險。因應對策如下：

1.透過良善且兼顧機密、完整及可靠性的網路架構設計，區隔作業環境及交易系統。

2.除交易需求外，避免儲存使用者資料及交易相關訊息，機敏資料之儲存及傳輸必須加密，且須符合密碼複雜度並選取適當加密演算法。

3.建立系統安全開發及維護程序，定期或不定期進行稽核、資安健診、風險評鑑以及災害復原演練等項目，持續降低系統風險。

4.建立身分驗證程序，存取權限之授予以必要性 (Need to know) 為原則，並留存及保護軌跡紀錄。

5.定期監控及測試網路安全現況，以發掘並修補網路弱點等。

(二)交易安全：

1.外部反洗錢/反套現因應對策：建立偵測系統，設定風險分析模組與指標，分析使用者的消費習慣、消費時間、消費額度、消費地點及常用金融機構帳戶等正常交易行為基準資料，一旦發現可疑之異常交易行為，立即告警，並通知相關人員妥善處理。

2.內部反詐欺：

(1)強化交易平台之資安防禦，依據相關法規所訂定之安全基準，定期執行資訊安全評估作業，即時發現安全弱點及潛在威脅。

(2)強化系統紀錄留存與證據保護能力，規劃系統紀錄之留存機制，集中管理各應用系統、作業系統、資料庫、網路設備及資安設備之紀錄及稽核軌跡並設定適當的告警指標，進行異常紀錄分析，以隨時掌握企業之資訊安全現況。

(3)建立完整之內控稽核制度。

三、請詳述裝設 Wi-Fi 無線網路路由器的應注意事項，以降低無線上網的資安風險。（25 分）

答題關鍵	無線網路的種類、區域劃分、通訊協定以及資安設定是基本的題型，建議可透過無線網路有別於有線網路的特性、通訊協定訊號範圍、連線時身份驗證機制以及軟硬韌體各項與資安相關之設定，回答本題。

【擬答】

(一)無線上網資安風險

因 WLAN 可將組織之網路延伸到控制範圍之外，例如：802.11b 若在室內有較多掩體阻擋無線電波，至多從廣播點向外延伸 100 公尺，室外則為 300 公尺。且經由 OTA(Over the Air)網路封包側錄 OTA(Over the Air)已非難事，攻擊者可透過啟用網卡的混雜模式(promiscuous mode)擷取無線網路流量，進而取得組織內部機敏資訊，常見針對無線上網的攻擊手法如下：

1.攔截 WLAN 傳輸之資料，造成資訊外洩

2.組織成員誤連上攻擊者偽裝的 WLAN 裝置，從而暴露在中間人攻擊(Man-in-the-Middle Attack)威脅之下

(二)無線網路路由器設定應注意事項

1.開啟自動韌體更新。

2.關閉 UPnP 和 WPS。

3.透過連線設備白名單(MAC 位址過濾)，鑑別(Authentication)連線之使用者與裝置，防止未授權者得到網路之存取權。

4.使用加密之應用服務或通訊協定，如 Internet Protocol Security(IPSec)，保護資料之機密性(Confidentiality of Data)，資料即使被攔截也無法知悉內容。

5.設定 Wi-Fi 驗證密碼時需要滿足密碼設定原則。

6.設定 Wi-Fi 加密協定(從上到下，安全性依次降低)：

(1)WPA2 + AES

(2)WPA + AES

(3)WPA + TKIP

(4)WEP

7.不使用預設網路名稱(SSID)，且可以設定無線網路路由器不廣播網路名稱，改以手動輸入網路名稱的方式請求連線。

四、電力分析（Power Analysis）是嘗試破解儲存於硬體密碼模組內的安全參數（Security Parameters）或密鑰（Secret Key）的常見攻擊手法之一。請詳述電力分析攻擊的原理及防禦方式。（25 分）

答題關鍵	電力分析破密算是比較特別的攻擊手法，類似的還有透過鍵盤餘溫、觸控螢幕上的汙痕猜出密碼等等，準備此類型的考題需要平時就有看資安相關新聞或論壇的習慣，並且彙整一些解題關鍵字，例如：本題是「能量消耗特徵」，把握關鍵字之後盡可能寫出手法和防禦方式。

【擬答】

(一)電力分析攻擊的原理

電力分析攻擊的基本原理是利用密碼設備執行過程中的電力洩露資訊與其所處理被攻擊中間值之間的統計依賴性恢復出密碼設備所使用金鑰。這種攻擊利用的是密碼設備的能量消耗特徵，而非密碼算法的數學特性。比如在晶片工作狀態下，探測晶片的電力消耗後再將加密過程中電路能量消耗與運算元關聯，進而用統計方法來取得金鑰。

(二)電力分析攻擊的防禦方式

1.隱藏技術

其基本想法為消除能量消耗的數據依賴性，要不將算法的執行過程隨機化，不然就是將設備的能量消耗特徵改變。改變能量消耗的方法有：

(1)採用使每個操作都消耗相同能量的方式製造設備。

(2)採用使設備能量消耗或多或少的隨機方式製造設備。

2.掩碼技術

亦稱為「遮罩技術」，指的是將一串二進位數字，通過與目標數字的按位元操作，達到封鎖指定位而實現需求。