基本資料

A1、學 校 名 稱：_____(全名)

A2、機 關 名 稱：_____(全名)

A3、資通安全責任等級：○ A ○ B ○ C ○ D ○ E

A4、姓　　名：_____

A5、公 務 電 話：_____ 例：02-00000000#000

A6、公 務 E - Mail：_____

A7、職　　務：○ 資訊主管 ○ 資訊人員 ○ 資安人員 ○ 機關之資安專職人員 ○ 其他，請註明 _____

策略面

* 1.1.請問108年資訊/資安預算?

	資訊 (含資安)	資安
預算經費 (千元)		

* 1.2.請問108年編列採購資安產品(含服務) 預算

	採購資安產品 (含服務)	其中國內資安產品 (含服務)
預算經費 (千元)		

* 1.3.請問108年資安預算比107年資安經費的增減情形

○ 1. 增加未達 5%

○ 2. 增加 5%~未達 10%

○ 3. 增加 10%~未達 15%

○ 4. 增加 15%~未達 20%

○ 5. 增加 20%及以上

○ 6. 相同

○ 7. 減少未達 5%

○ 8. 減少 5%~未達 10%

○ 9. 減少 10%~未達 15%

○ 10. 減少 15%~未達 20%

○ 11. 減少 20%及以上

○ 12. 不知道

* 1.4.請問109年將新增採購下列哪些是最急迫需採購的資安產品(含服務)？（選擇數量上限：5個）

選項說明

▲防毒：由軟體或硬體來實作，用於偵測入侵電腦的病毒、蠕蟲、木馬與惡意程式，通常含有即時程序監控識別、惡意程式掃描與清除及自動更新病毒資料庫等功能。
▲防火牆：由軟體或硬體來實作，利用系統所建立的網路/應用程式安全性規則，有效的控制對內與對外的安全存取機制。
▲郵件過濾裝置：過濾垃圾郵件以達到資訊安全防護的裝置。
▲入侵偵測系統(IDS)：可以偵測外部及內部人員對未經授權之資訊系統做不正當的存取或攻擊，可提供紀錄以供審核及事後追蹤。
▲入侵防禦系統(IPS)：為入侵偵測系統的延伸，除了偵測外也能發揮主動防禦的功能，如刪除垃圾封包、擋掉入侵IP等等。
▲網站應用程式防火牆(WEF)：針對網站的常見攻擊進行防禦，諸如跨網站攻擊(cross-site scripting)以及SQL injection攻擊。
▲進階持續性滲透攻擊(APT)防禦：針對特定組織所作的複雜且多方位的網路攻擊防護。
▲資料外洩防護(DLP)：透過內容比對偵測技術，以管控資料的外洩防護。
▲數位版權管理(DRM)：用來保護數位內容使用的管理機制，透過加密認證等過程，確認是合法使用數位內容之使用者，可在文件上加浮水印、限制使用時間、使用載具限制、取得授權等方式來保護數位內容。

▲日誌管理(Log Management)：蒐集及分析資訊系統或設備在連線和運作時所產生的紀錄，讓IT人員能夠監控系統的運作狀態，了解資料存取行為和使用者的作業活動，以及是否有異常情況發生等項。
▲資料庫監控(DAM)：記錄所有資料庫的存取軌跡，以監控與稽核資料庫活動。
▲行動裝置與應用管理(MDM/MAM)：針對行動裝置，如手機、平板進行裝置功能的控管，或是資料儲存管理。前者例如鎖定照相功能、限定可安裝的應用程式，後者如電子郵件管理、聯絡人資訊、或是可存取的文件等。
▲資安健診服務：透過整合各項資通安全項目的檢視服務作業，提供受檢機關資安改善建議，藉以落實技術面與管理面相關控制措施，以提升網路與資訊系統安全防護能力。
▲資安監控中心(SOC)：由資安人員、管控系統平台、管控程序，三者加以整合而成。其中的系統平台即為資安事件管理平台，通常具備事件偵測、事件收集、知識庫、事件分析、回應與通報等基本功能。
▲弱點掃瞄服務：檢測系統潛在弱點，並依據檢測結果提出改善建議，協助受測目標提升系統安全防護。
▲滲透測試服務：IT人員透過模擬駭客的攻擊方式，進行滲透或穿透跳躍主機之入侵測試，設法取得未經授權之存取權限，並測試內部資訊是否有遭受不當揭露、竄改或竊取之情況。
▲社交工程郵件測試服務：模擬駭客寄送社交工程信件給受測對象，以信件之標題及內容引誘收件人「開啟信件」、「點閱連結」或「開啟附件」進而下載惡意程式的攻擊行為，進而統計分析。
▲資安鑑識服務：遭遇資安事件的後續處理，進行證據的收集與追蹤分析。
▲行動化應用軟體資安檢測服務：為了防範Mobile Application或Mobile App 被駭，所執行之安全檢測作業。

○1. 防毒

○2. 防火牆

○3. 郵件過濾裝置

○4. 入侵偵測/入侵防禦系統 (IDS/IPS)

○5. 網站應用程式防火牆 (WEF)

○6. 進階持續性滲透攻擊 (APT) 防禦

○7. 資料外洩防護 (DLP)

○8. 數位版權管理 (DRM)

○9. 日誌管理 (Log Management)

○10. 資料庫監控 (DAM)

○11. 行動裝置與應用管理 (MDM/MAM)

○12. 資安健診服務

○13. 資安監控中心 (SOC)

○14. 弱點掃瞄服務

○15. 滲透測試服務

○16. 社交工程郵件測試服務

○17. 資安鑑識服務

○18. 行動化應用軟體資安檢測服務

○19. 其他，請註明 _____

○20. 以上皆無

○21. 不知道

管理面

* 2.1.請問全部核心資通系統導入及通過CNS 27001或ISO 27001第三方驗證，並持續維持其驗證有效情形

○ 1. 全部符合

○ 2. 多數符合

○ 3. 半數符合

○ 4. 少數符合

○ 5. 全部不符合

* 2.2.請問全部核心資通系統造成最嚴重影響的無法導入及通過CNS 27001或ISO 27001第三方驗證之原因(已全部導入及通過可免填)（選擇數量上限：3個）

○1. 經費不足

○2. 實體環境限制

○3. 尚未全部導入但已規劃辦理

○4. 人力不足

○5. 內部人員能力不足

○6. 委外廠商能力不足

○7. 其他業務單位反彈

○8. 不受長官重視

○9. 其他，請註明 _____

○10. 自行評估無需要導入

* 2.3.請問員工人數

選項說明

▲現有員工總數：包括編制內與約聘僱人員等，不含短期臨時人員、一般性工友、司機、警衛及學生。
▲公務機關請填專職人員。

	員工總數	資訊人員(含資安人員)	資安專職人員
人數			

* 2.4.請問資安專職人員身分

選項說明

▲現有員工總數：包括編制內與約聘僱人員等，不含短期臨時人員、一般性工友、司機、警衛及學生。
▲公務機關請填專職人員。

	正職資安人員	資安約聘及約僱人員	資安委外或其他人力(含職代)	已配置資安正職員額但尚未任職	已配置資安約聘僱員額但尚未任職
人員					

技術面

* 3.1.請問目前已採購下列哪些資安產品(含服務)（選擇數量上限：無限個）

○1. 防毒

○2. 防火牆

○3. 郵件過濾裝置

○4. 入侵偵測/入侵防禦系統 (IDS/IPS)

○5. 網站應用程式防火牆 (WEF)

○6. 進階持續性滲透攻擊 (APT) 防禦

○7. 資料外洩防護 (DLP)

○8. 數位版權管理 (DRM)

○9. 日誌管理 (Log Management)

○10. 資料庫監控 (DAM)

○11. 行動裝置與應用管理 (MDM/MAM)

○12. 資安健診服務

○13. 資安監控中心 (SOC)

○14. 弱點掃瞄服務

○15. 滲透測試服務

○16. 社交工程郵件測試服務

○17. 資安鑑識服務

○18. 行動化應用軟體資安檢測服務

○19. 其他，請註明 _____

○20. 以上皆無

○21. 不知道

* 3.2.請問最擔心遭遇下列哪些可能造成嚴重影響的資安威脅？（選擇數量上限：2個）

○1. APT攻擊竊取機密資料

○2. DDoS攻擊癱瘓網路運作

○3. IoT設備資安弱點威脅升高

○4. 關鍵資訊基礎設施遭受攻擊

○5. 網路與資訊服務中斷

○6. 資安(訊)供應商持續遭駭破壞供應鏈安全

○7. 人力不足

○8. 內部人員能力不足

○9. 委外廠商能力不足

○10. 個資外洩

○11. 以上皆不擔心

○12. 其他，請註明 _____

* 3.3.請問資訊設備(含軟、硬體、網路設備、其他資訊設備)導入資訊資產管理系統的情形

○ 1. 有，請註明品牌 _____

○ 2. 沒有

* 3.4.請問107年遭遇資安事件，其發生來源為何？（選擇數量上限：無限個）

○1. 外部攻擊(駭客)

○2. 內部人員疏失

○3. 離職人員或內部犯罪

○4. 委外供應商

○5. 不知道

○6. 其他，請註明 _____

* 3.5.請問107年遭遇的資安事件的類型（選擇數量上限：無限個）

選項說明

▲符合貴機關在通報應變網站通報的資安事件

○1. 網頁攻擊(DEF) - 網頁置換

○2. 網頁攻擊(DEF) - 惡意留言

○3. 網頁攻擊(DEF) - 惡意網頁

○4. 網頁攻擊(DEF) - 網頁木馬

○5. 網頁攻擊(DEF) - 釣魚網頁

○6. 網頁攻擊(DEF) - 網站個資外洩

○7. 非法入侵(INT) - 系統遭入侵

○8. 非法入侵(INT) - 植入惡意程式

○9. 非法入侵(INT) - 異常連線

○10. 非法入侵(INT) - 異常連線

○11. 非法入侵(INT) - 垃圾郵件 (Spam)

○12. 非法入侵(INT) - 資料外洩

○13. 阻斷服務(Dos/DDos) - 服務中斷

○14. 設備問題 - 設備故障/損毀

○15. 設備問題 - 電力異常

○16. 設備問題 - 網路服務中斷

○17. 設備問題 - 設備遺失

○18. 其他，請註明 _____

○19. 沒有遭遇資安事件

* 3.6.請問107年遭遇資安事件造成哪些損失（選擇數量上限：無限個）

○1. 沒有損失

○2. 個資或資料外洩

○3. 財務損失

○4. 信譽損失

○5. 無法估計

○6. 不知道

○7. 其他，請註明 _____

安全系統發展生命週期（SSDLC）

* 4.1.根據資通安全責任等級分級辦法之資通系統防護基準，有系統防護需求分級為「高」之資通系統(無論自行開發或委外)

○ 1. 有（續答）

○ 2. 沒有(請跳填問項4.3)（跳答 - 4.3.其他系統防護需求分級之資通系統(自行開發或委外)，在開發流程中，是否導入SSDLC?）

4.2.系統防護需求分級為「高」之資通系統(自行開發或委外)，在開發流程中，是否導入安全系統發展生命週期(SSDLC)

○ 1. 全部符合

○ 2. 多數符合

○ 3. 半數符合

○ 4. 少數符合

○ 5. 全部不符合

* 4.3.其他系統防護需求分級之資通系統(自行開發或委外)，在開發流程中，是否導入SSDLC?

○ 1. 全部符合

○ 2. 多數符合

○ 3. 半數符合

○ 4. 少數符合

○ 5. 全部不符合

4.4.請問全部資通系統(自行開發或委外) 無法導入SSDLC最嚴重影響的原因？ (已全部導入可免填)（選擇數量上限：3個）

○1. 經費不足

○2. 實體環境限制

○3. 尚未全部導入但已規劃辦理

○4. 人力不足

○5. 內部人員能力不足

○6. 委外廠商能力不足

○7. 其他業務單位反彈

○8. 不受長官重視

○9. 其他 _____