



資通安全業務重點工作

114年6月



大綱

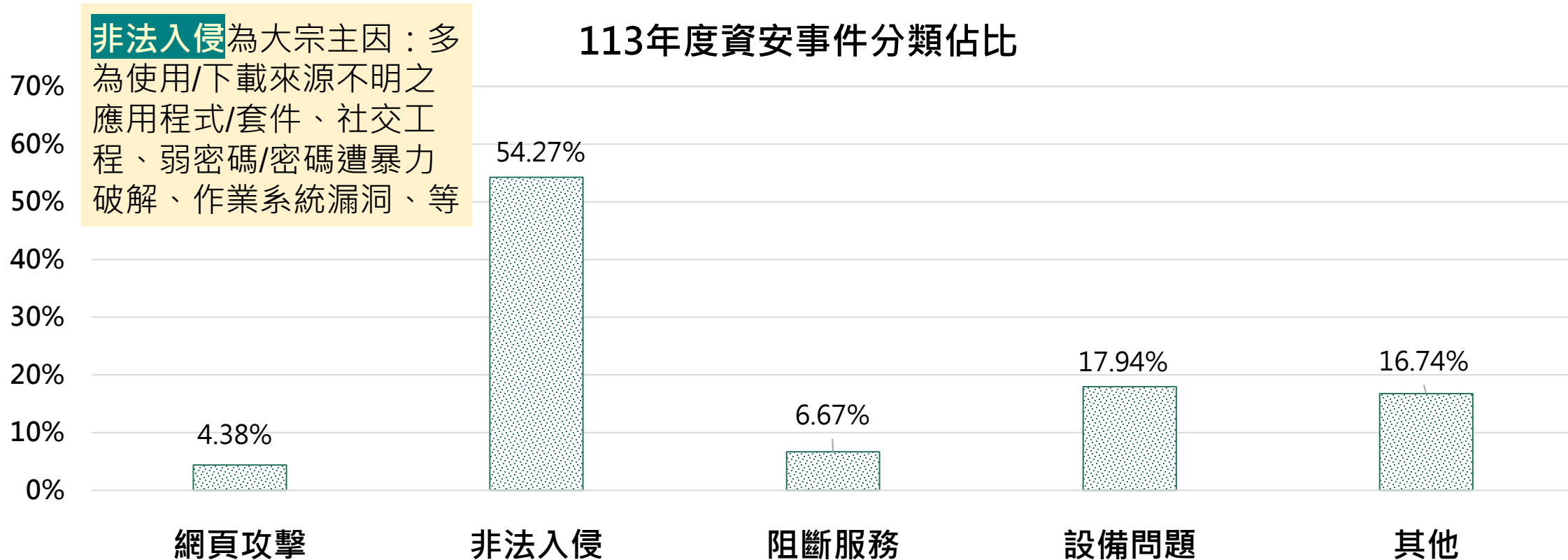
- 一、113年政府資安威脅分析與建議防範措施
- 二、113年資安稽核與網路攻防演練
- 三、資安法規遵循事項
- 四、第七期國家資通安全發展方案(114年至117年)
- 五、資安人才培育
- 六、危害國家資通安全產品重點工作

一、113年政府資安威脅 分析與建議防範措施



113年納管機關資安事件通報統計

年度	事件數	1級事件	2級事件	3級事件	4級事件
113年	914	749	147	18	0





113年3級以上資安事件樣態

影響	發生原因
機密性 (共9件)	● <u>網站查詢權限設定不當</u>，供應商未依規格書撰寫程式致個資外洩。(計1件) ● <u>網站存在系統漏洞</u>，攻擊者可利用漏洞取得個資。(計1件) ● <u>供應商遭駭</u>：駭客透過廠商VPN帳號進入機關系統查詢個資。(計1件) ● <u>社交工程</u>：機關同仁因社交工程導致帳密遭到竊取，駭客並利用該帳密登入內部系統取得個資。(計1件) ● <u>人員疏失</u>： 誤將未遮蔽之個資公開、誤上傳民眾之個資於公開網站、辦理活動未將敏感資訊遮蔽、將含有個資資料寄送給民眾、誤將機敏資料上傳至公開網站等。(計5件)
可用性 (共9件)	● <u>機房起火致設備異常</u>，因電力室內之配電盤燒毀，造成網路內外服務中斷。(計1件) ● <u>資料庫主機異常及設定問題</u>，導致HIS醫療資訊系統無法作業使用。(計2件) ● <u>市電瞬斷影響核心系統可用性中斷</u>。(計1件) ● <u>全球性當機</u>，影響機關CI核心業務可用性(計5件)



資安事件案例-供應商遭駭

駭客利用**廠商VPN帳號**登入後，再透過機關人員帳號進入系統查詢病患資料，致個資外洩，通報3級資安事件。



建議防範措施

- 對於每一種允許之遠端存取類型，均應**先取得授權，建立使用限制、組態需求、連線需求及文件化**。
- 機關應加強遠端存取控制機制，依「**原則禁止、例外允許**」方式辦理
- 若需允許外部遠端維護，應加強防護措施，如採VPN並啟用**多因子認證機制**等，以強化遠端登入身分鑑別。



資安事件案例-機敏資訊上傳公開網站致外洩

某縣政府接獲協力廠商告知該府**SOC月報**疑似遭上傳至VirusTotal網站，內容包含該府網段資訊等**機敏資訊**，經查為該府**SOC廠商不慎將該報告上傳至網站上**，致機敏資料外洩，爰通報3級資安事件。



強化措施參考

- 確認資料機敏性資料，**避免將機敏資訊上傳至公開系統**。
- 如需透過VirusTotal等服務檢查是否為惡意檔案，可**透過檔案Hash值檢查**。
- **針對文件機敏性分級**，如設置TLP (Traffic Light Protocol)分級。
- 注意廠商委外管理，針對機敏資訊應加強管理與防護。

二、113年資安稽核與 網路攻防演練

113年資安稽核共同發現事項

策略面



- 業務持續運作演練未納入業務單位角色，範圍未涵蓋全部核心系統
- 管審會議出席率偏低，且未由各業務單位主管親自出席

管理面



- 資訊系統或資訊資產漏未盤點，如未完整納入OT或IoT設備
- 資安要求未完整訂於RFP或契約書

技術面



- 弱點掃描等安全性檢測，複測後仍有高風險漏洞，且未有相關弱點修補紀錄
- 未落實遠端連線「原則禁止、例外允許」管理原則



113年網路攻防演練常見弱點說明

- 針對主要弱點類型列出**前3名**常見發現事項樣態及案例

1



加密機制失效

機敏資料外洩

2



注入攻擊

注入漏洞

3



無效存取控管

限制存取功能失效



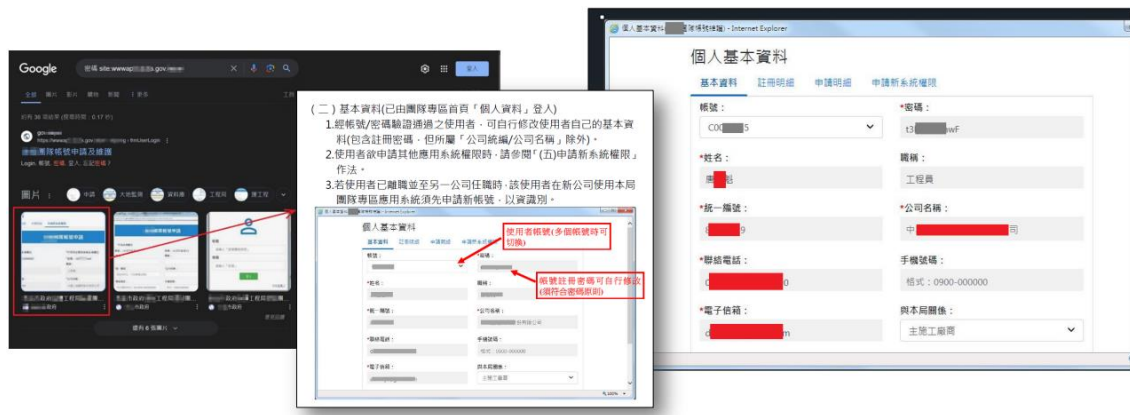
機敏資料外洩

樣態

系統說明文件洩漏帳號通行碼或個人資料等機敏資訊

案例

透過Google Hacking查找系統申請帳號之操作說明，並使用PDF軟體複製圖片，發現原已遮罩之帳號通行碼



檢測方式

透過PDF軟體複製圖片檢視敏感資料是否遮罩

姓 名	獎 金	姓 名	獎 金
王 明	0,000	王 大明	98,000
陳 壯	0,000	陳 大 壯	88,000
林 美	0,000	林 小 美	78,000

改善建議

透過Windows系統「剪取工具」合併圖層來遮罩敏感資料





注入漏洞(XSS攻擊)

樣態

網站**未妥善處理輸入內容**，可輸入惡意指令並當成**javascript**語句執行

案例

嘗試於網頁上欄位輸入攻擊語法成功觸發XSS攻擊語法，並顯示攻防演練圖示

【忘記密碼】

市縣： 02-台北

帳號： admin"><img src=https://i.imgur.com/xl

E-Mail： test@a.a

驗證碼： 8086 8086 ok

輸入資訊不正確，請重新輸入

【忘記密碼】

市縣： 請選擇

帳號： admin

E-Mail： test@a.a

驗證碼：

網路攻防演練



檢測方式

透過以下常見XSS語法輸入於網頁輸入框進行驗證：

1. `<script>alert('XSS')</script>`
2. `"><script>alert('XSS')</script>`



改善建議

在伺服器端網頁程式對輸入之參數進行過濾，避免使用者輸入任何 Script 程式碼及資料庫語法



注入漏洞(SQL Injection)

樣態

網站使用URL傳遞查詢條件，例如
`http://x.x.x.x/products.php?id=123`，可透過工具獲取潛在資訊

案例

目標網頁，發現網址參數「G」為網頁應用程式中的 SQL 注入點，進行 Query。

資料提供者

縣市

生

檢測方式

透過SQL Injection檢測工具進行資料庫內容**枚舉與提取**，取得使用者、密碼雜湊、權限、角色、資料庫、資料表和資料列。

```
[13:32:54] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[13:32:54] [INFO] starting dictionary-based cracking (sha256_generic_passwd)
[13:32:54] [INFO] starting 16 processes
[13:35:19] [WARNING] no clear password(s) found
Database: [REDACTED]
Table: adminuser
[7 entries]
```

UserID	State	Password	UserName	UserRank
3	N	00DPAMQKNs	cUTxUYu3Bw=	R
7	Y	5RwQxNN0+a	PrrMwDXJVU=	A
2	Y	jwN6TVn1Tw	t0D7jv3HgM=	R
4	Y	wLQKhZUhD7	h8dubpT3/c=	A

改善建議

- 1.使用**參數化查詢**或預處理語句將 SQL 語句和使用**使用者輸入的數據分開處理**。
- 2.過濾或**轉譯特殊字符**：如單引號 '、雙引號 "、分號 ;、等號 =、註解符 --、/* 等。



限制存取功能失效

樣態

未限制存取來源或無權限控管，導致任一使用者皆可存取特定頁面

案例

瀏覽網站複製檔案下載連結，並嘗試修改路徑，成功取得系統非機敏且非公開資料



檢測方式

逐一頁面進行權限控管檢查，依系統角色差異，明確區分存取來源為訪客(未登入)、一般使用者及管理者等權限

	系統負責人	系統管理員	一般使用者	訪客
指派/取消管理員	○	×	×	×
編輯專案公告	○	×	×	×
編輯系統資訊	○	×	×	×
新增/刪除成員	○	○	×	×
檢視專案資訊	○	○	×	×
檢視系統資訊	○	○	×	×
上傳檔案	○	○	○	×

改善建議

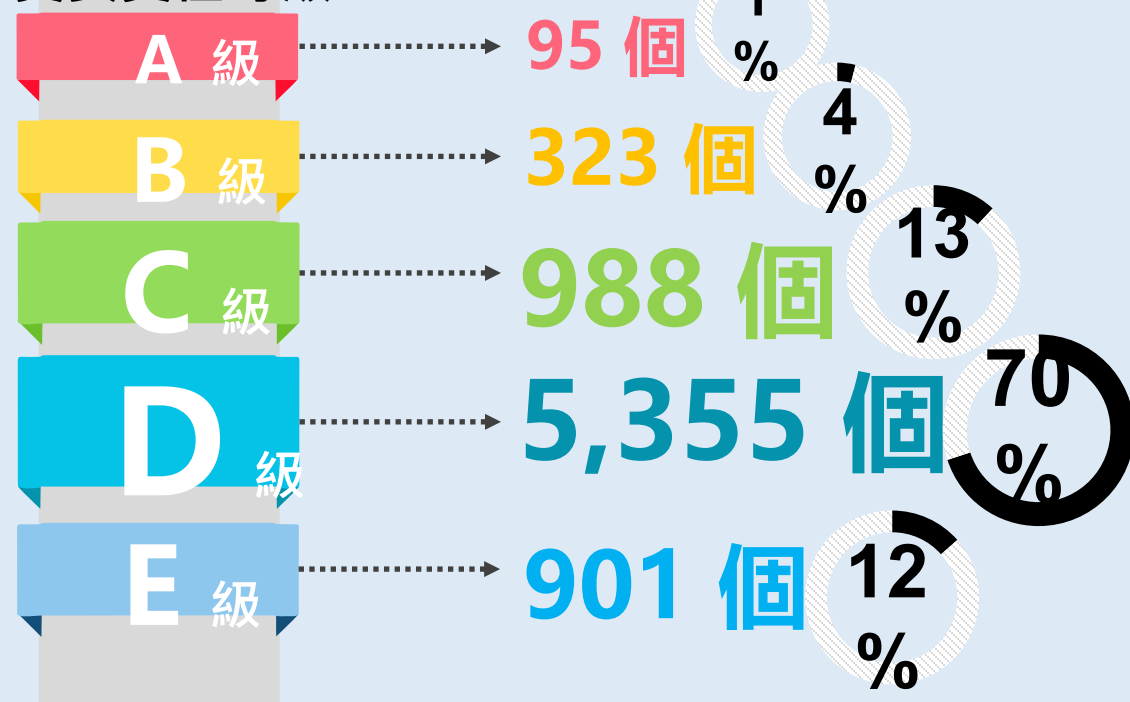
避免不當人員存取系統或機敏資料，應設定資料存取權限控管，加強路徑驗證，實施最小權限原則

三、資安法規遵循事項

2年1次資安責任等級重新核定

目前納管情形

資安責任等級



總計7,662個納管機關(包含公務機關及特定非公務機關)

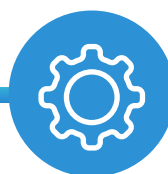
依據資通安全責任等級分級辦法§3規定，公務機關應**每二年**提交自身、所屬(監督)或所轄公務機關，與所管特定非公務機關之資通安全責任等級

規劃期程



5-6月

通函
各機關提報



7-8月

審查



9月

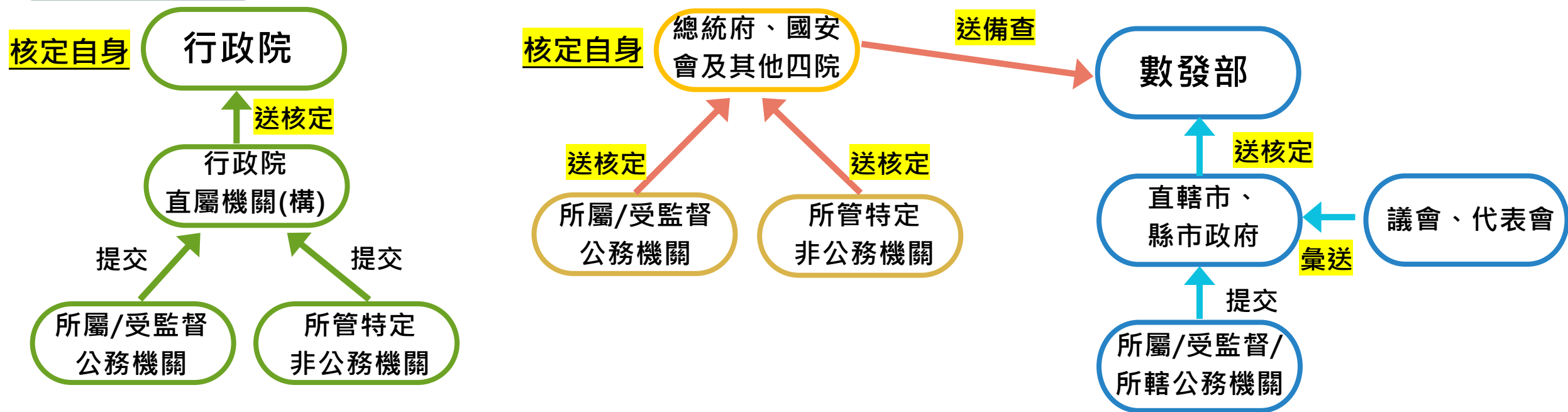
核定
(備查)

✓ 5月23日函請各機關於**6月30**日前完成**提報**作業



資安責任等級提報

提報程序



注意事項

- ✓ 行政院所屬機關函送**行政院**核定
- ✓ 地方政府應送**數位發展部**核定；府會及其他四院送**數位發展部**備查
- ✓ **地方議會**應由**地方政府**統一彙送
- ✓ 原則每2年核定一次，如有新設、裁撤或資通業務調整者，請於**1個月內完成提報**

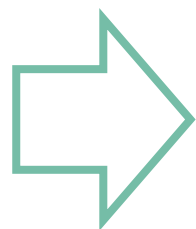


資安責任等級認定

✓ 各機關維運自行或委外設置、開發之資通系統，其資安責任等級應至少為C級以上

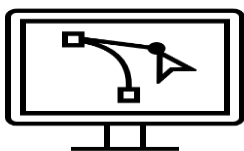
參考資訊

請上級及中央目的事業主管機關依相關資料核實審認



管考系統-
系統清冊

✓ 參考維護計畫實施情形機關自行維運系統清冊



政府資訊
採購網

✓ 政府電子採購網之系統開發、維運委外案



資安事件

✓ 因機關維運系統通報之資安事件



中長程計畫

✓ 機關提出之系統開發計畫案



應辦事項常見問題

資通安全弱點通報機制

資安法常見問題4.14

- **定期上傳**以比對弱點資訊，並針對發現弱點設定修補期限
- 弱點未能如期修補時，應於完成修補前**規劃緩解措施**
- 相關**弱點處置方式**或改善措施，建議完成比對弱點後至**VANS系統（更新）填寫**，強化機關弱點管控作為

SOC監控提交資料

資安法常見問題4.21

- 各機關依國家資通安全研究院網站公告之「政府領域聯防監控作業規範」辦理提交，並即時回傳「**資安監控單**」及「**情資分析單**」，另於**每個月5日前**回傳上個月的「**監控設備狀況單**」

EDR提交資料方式

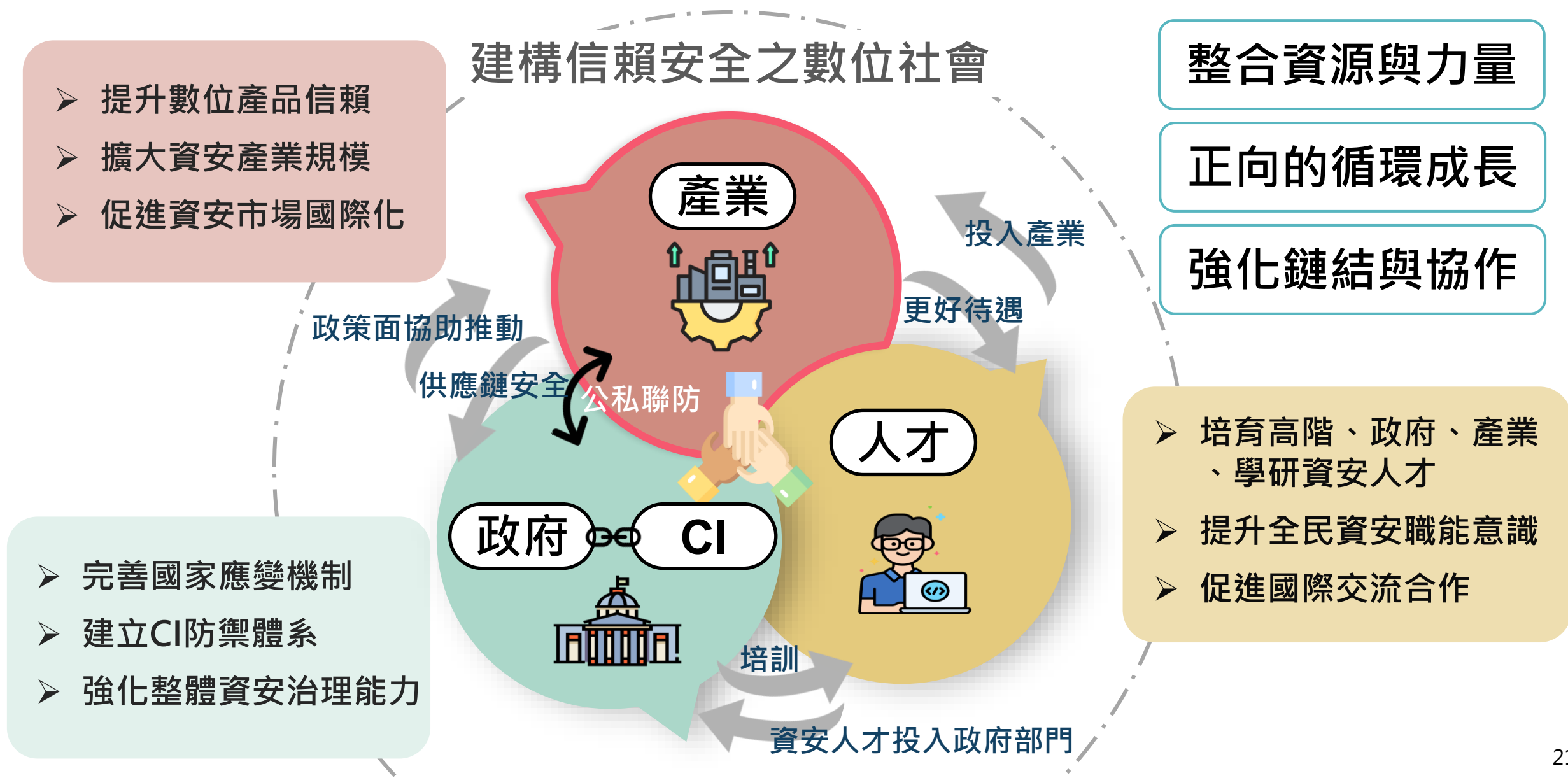
資安法常見問題4.16

- 經EDR端點掃描告警資訊並分析確認為**資安事件**後，依國家資通安全研究院網站公告之「資料回傳格式說明」，透過SOC回傳管道提交至主管機關
- 機關可查看回傳之「**監控設備狀況單**」是否含EDR設備，確認上傳機制正常運作

四、第七期國家資通 安全發展方案 (114年至117年)



第七期國家資通方案核心價值





第七期國家資通安全發展方案框架

扣合戰略2025

策略一

全社會資安防禦

- 1-1 完善國家資安應變機制
- 1-2 提升全民資安職能及意識
- 1-3 建構全社會資安防護網

...

策略三

壯大我國資安產業

- 3-1 推動資通產品檢測制度
- 3-2 強化政府採購供應鏈風險管理
- 3-3 擴大資安產業規模並向國際輸出



推動策略與具體措施



願景

建構信賴安全之數位社會



目標

- ✓強化全社會資安防禦韌性
- ✓豐富資安產業生態系
- ✓構築新興科技防禦技術

策略二

提升關鍵基礎設施資安韌性

- 2-1 建立關鍵基礎設施資安防禦體系
- 2-2 提升關鍵基礎設施資安聯防能量
- 2-3 精進關鍵基礎設施資安治理能力

...

策略四

AI新興資安科技應用與合作

- 4-1 拓展AI技術應用以提升資安防護能量
- 4-2 強化新興資安科技前瞻研究
- 4-3 促進國際資安交流合作

...

五、資安人才培育



資安攬才育才推動規劃

擴大人力進用管道

非資訊處理職系 現職公務人員轉任

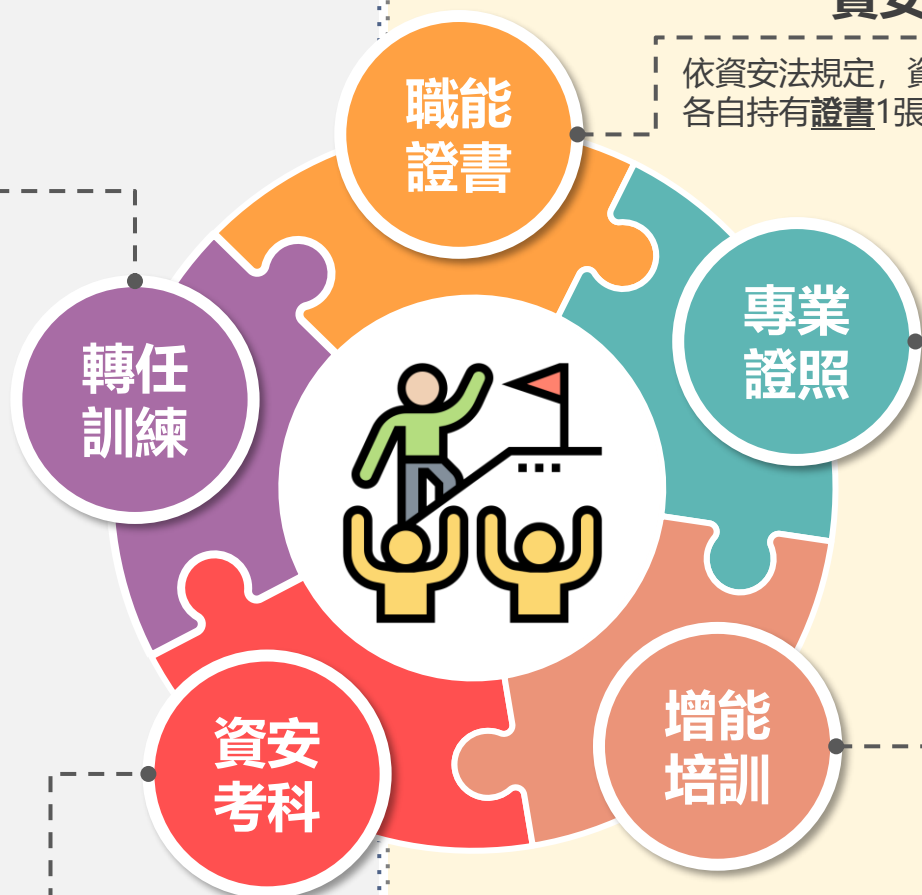
目標培訓450人(得視預算核撥情形調整)，優先投入政府資安工作

政府資安人力職 能轉換訓練計畫

高考三級新增資 通安全類科

透過國家考試取才

包含資通安全概論、資通安全管理、資通安全法令與規範、資通安全防護技術等4科專業科目



資安職能訓練

依資安法規定，資安專職人員應各自持有證書1張以上

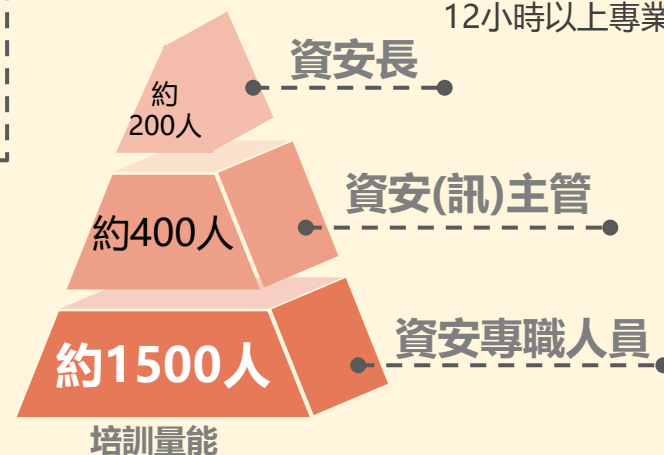
系統性人才培育 (職能奠基、增能培訓)

資安專業證照課程

依資安法規定，資安專職人員應各自持有證照1張以上

資安增能培訓

依資安法規定，資安專職人員每人每年應至少接受12小時以上專業訓練





資安職能評量精進措施

提升評量服務品質

擴增評量場地：增3處

提升評量頻率：每月

調整辦理方式：集中首複測、換證場次

桃園 - 新增
健行科技大學

台北 - 既有
中國文化大學
國家考場

台中 - 既有
國立中興大學

花蓮 - 新增
慈濟大學

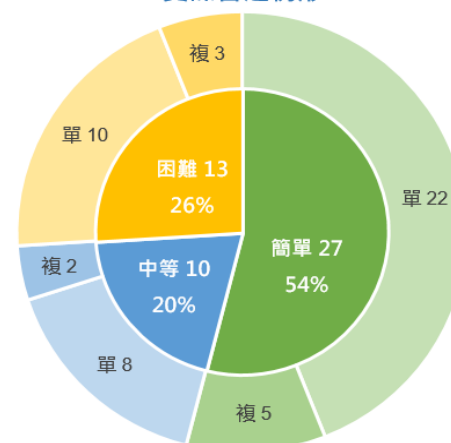
台南 - 既有
崑山科技大學

高雄 - 新增
輔英科技大學

優化評量試題

- ✓ 統計評量結果
- ✓ 檢討成績分布
- ✓ 分析難易度及鑑別度

實際答題情形



參測人數	通過率	平均分數
20	70.00%	71.20



資通安全概論教材改版

編修教材

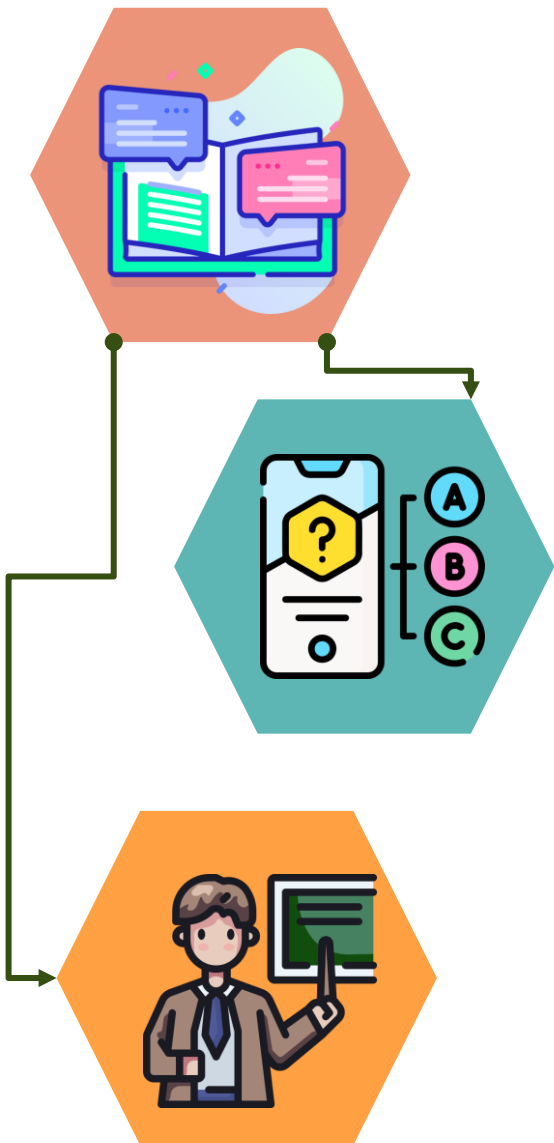
- 發展教科書式教材
- 扣合《資通安全管理法》與共通規範文件
- 預計115年起改用新版教材

命題作業

- 配合教材更新內容，啟動命審題
- 檢視試題疑義，汰換不適宜試題

師資培訓

- 資安職能訓練機構講師
- 說明改版教材重點





資安專職人員增能培訓

資安數位課程(專業)

資安人員專業訓練
(1年10~20場次)

分區調訓資安責任等級
A、B、C級公務機關之資
安專職人員

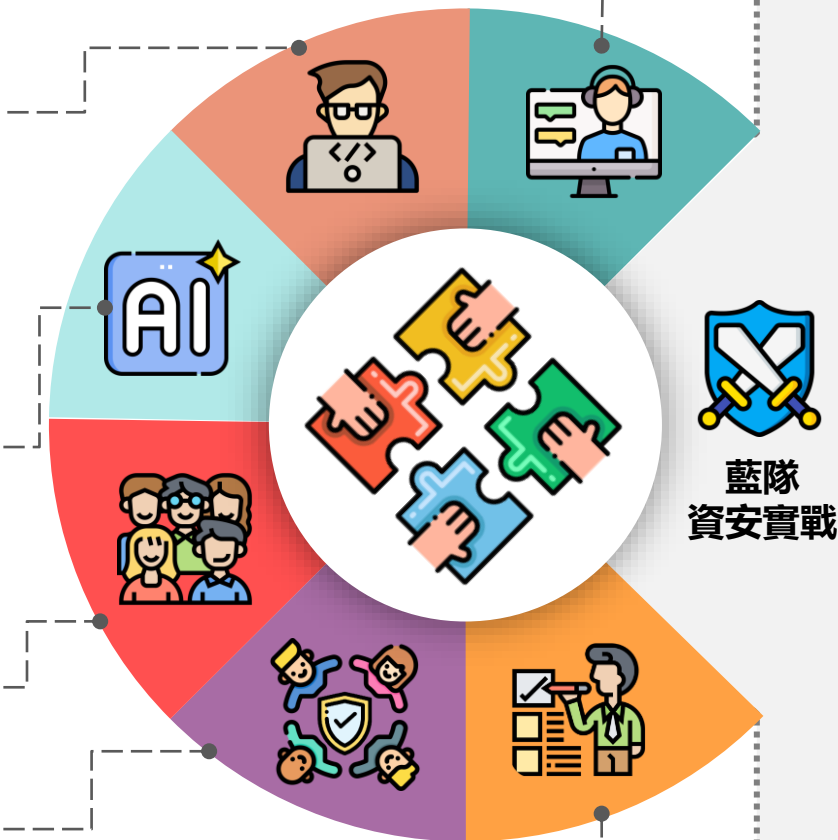
新興資安訓練

AI♥資安學院課程：
預定114年7月~9月辦
理，以公餘時間為主，
協助政府資安人員瞭解
AI在資安領域之應用

資安菁英培訓課程

政府資通安全防護
巡迴研討會

稽核員訓練



註：綠底項為特定非公務機關可用訓練資源

授課對象

資通安全管理法納管機關現職資安人員，擔
任**技術面**職務之資安專職(責)人員為主

課程日期及地點

預計**114年10月下旬**開辦兩期，每期各一天
臺北電腦教室

授課方式

講授教學

上機**實作演練**(AD環境安全檢測與強化)

課程內容

資安**藍隊**核心概念

AD基礎架構與安全模型及常見攻擊手法

藍隊防禦演練與實作

六、危害國家資通安全 產品重點工作



危害國家資通安全產品限制使用原則與相關規定

01 行政規則

發布日期：108 年 4 月 18 日

依「**危害國家資通安全產品限制使用原則**」，倘因業務需求且無其他替代方案，應具體敘明理由，經**機關資安長**及其**上級機關資安長**逐級核可，**函報數位發展部核定**後，以**專案方式購置列冊管理**，及遵守以下規定：

1. 指定特定區域及特定人員使用
2. 使用理由消失應立即停止使用
3. 以**不含個資及資料的電腦單機**將其下載並以斷網或非公務網路之獨立網路使用較為安全

02 行政函釋

函文日期：109 年 12 月 18 日

為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，行政院秘書長109年12月18日院臺護長字第1090201804A號函知各機關，**公務用之資通訊產品不得使用大陸廠牌(包含軟體、硬體及服務)**。

專案申請案例

中央及地方政府警政單位，因鑑識需求且無其他替代方案，規劃採購與使用**大陸廠牌監視器鑑識分析軟體**。



危害國家資通安全產品限制使用原則之限制範圍

各機關對危害國家資通安全產品限制使用原則【發布日: 108/04/08、修正日: 111/11/28】

限制
範圍

中央機關(構)

地方機關(構)

公立學校

公營事業

行政法人

各機關自行
或委外營運
，提供公眾
活動或使用
之場地

參考
辦理

中央目的
事業主管
機關

應督導

關鍵基礎設施提供者

政府捐助之財團法人



大陸廠牌之定義與認定方式

大陸廠牌之定義

「大陸廠牌」係指大陸地區廠商所提供之產品，至大陸地區廠商之定義係依行政院公共工程委員會107年12月20日工程企字第1070050131號函所稱「大陸地區廠商」包含大陸地區法律設立登記之公司、合夥或獨資之工商行號、法人、機構或團體。

大陸廠牌之認定方式

→ 由各機關「從嚴認定」。



機關辦理採購得依個案需求，評估與限制涉陸情形

工程會函釋

行政院公共工程委員會工程企字第1070050131號函釋 發布日期：112年12月20日

機關辦理資通訊產品採購，得依個案需求，限制涉陸情形：

01

得限制 陸製

可於投標須知明定廠商所提供之財物或勞務之原產地不得為大陸地區。

02

得限制 陸資

採購內容涉及國家安全者，可於投標須知載明，不允許大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與區。

實務案例與建議

- 案例1：某廠牌觸控筆**搭配使用APP**為大陸廠商開發。
- 案例2：某廠牌無人機為**第三地區含陸資成分廠商**。
- **建議**：機關辦理**資通訊產品(含硬體、軟體及服務)**採購時，**可依個案需求，審慎評估與限制涉陸情形**，以避免公務及機敏資料遭不當竊取。



工程會訂定「採購契約範本附記條款特別聲明」

工程會函釋

工程會114.5.20工程企字第1140100189號函訂定「採購契約範本附記條款特別聲明」

機關辦理各類採購時，契約如約定須交付書面履約成果者，應將「採購契約範本附記條款特別聲明」納入採購契約，重點摘述如下：

◆ **履約禁用DeepSeek(含禁止廠商使用DeepSeek製作書面履約成果)**：於特別聲明明定，契約如約定廠商須交付書面履約成果者，應禁止使用DeepSeek製作，並增訂通案之生成式AI使用條款，包含：「履約禁用中國大陸廠牌資通訊產品」、「不得提供公務機密予AI」、「使用AI履約須報機關同意」，**並輔以切結書規範廠商責任**。

◆ 廠商如違反上述禁用條款，機關得終止或解除契約。

【切結書範本】

使用資通訊產品禁制事項同意書/切結書
(得標後檢附)

本廠商(得標廠商)履行(採購機關)辦理之(標的名稱)案，已充分瞭解並遵行本特別聲明所定資通訊產品之禁制事項規範，於履約過程及履約標的均無違反前述禁制事項，如有違反，願賠償一切因此所生之損害，並擔負相關民、刑事責任。

立書人

投標廠商：(蓋章)

負責人：(蓋章)

中華民國 年 月 日



數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理