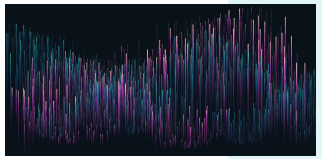


1

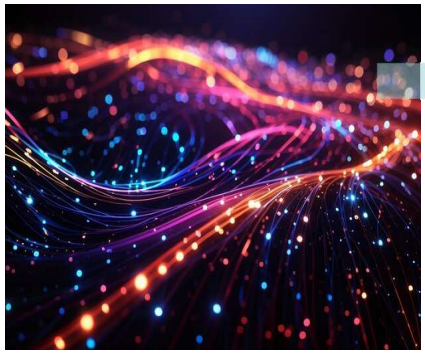
課程大綱



- 資訊安全暨個資隱私保護安全規定宣導
- AI 時代下的法規趨勢與資訊安全守則
- 近期資訊安全暨個資新聞
- Q & A 時間
- 隨堂測驗

2

2



一、資訊安全暨個資隱私保護安全規定宣導

- 資訊安全政策
- 隱私保護政策
- 新進人員個資保護宣導須知

3

3

資訊安全政策

■文件編號：YAN-ISMS-01-01資訊安全政策

■版次：2.2

■目的

延宇資訊股份有限公司（以下簡稱本公司）為強化資訊安全管理及個人隱私資料管理，確保所屬之資訊資產、個資資產的機密性、完整性及可用性，以提供本公司之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

4

4

資訊安全政策

■適用範圍

➢ 管理制度

本文件係根據本公司管理之需要，並參考ISO/IEC 27001:2022國際標準要求之規定製定，以滿足ISO/IEC 27001:2022國際標準認證之要求。

➢ 組織範圍

本文件適用於本公司各單位。

5

5

資訊安全政策

■**資訊安全政策**

➢ 本公司應指派資安長（個資管理代表）成立資訊安全暨隱私保護委員會，負責擬定本公司之資訊安全政策。本公司之資訊安全政策於本公司資安長（個資管理代表）審查核可後，發佈實施。本公司之資訊安全政策，包含資訊安全管理政策和資訊安全防護措施政策二個部分，**應每年定期或當發生重大變更時進行審查與維護**，說明如下：

1. 資訊安全管理政策

1.1 資安長（個資管理代表）應確保建立資訊安全政策和目標，且與本公司之營運策略方向相容。

1.2 本公司之資訊安全管理政策為之資訊安全管理政策為「**提供安全與持續運作之資訊系統操作、維護，確保資訊系統及資訊之安全，達成本公司資訊安全管理目標**」。

1.3 資訊安全政策之發佈更新，應讓本公司同仁知悉，並依據需求，讓關注方了解政策之要求。

6

6

資訊安全政策

2. 資訊安全防護措施政策

2.1 移動式儲存媒體管理政策：使用移動式儲存媒體儲存資訊，應先經核准；且不應儲存機密等級為「機密」之資訊。

2.2 遠距工作管理政策：經由外部網路連接本公司網路與資訊服務運作環境，應先經核准。

2.3 存取控制政策：使用者僅能存取和其工作相關之資訊系統與資訊；擁有特別存取權限之使用者，應限制存取權限之配置與使用。

2.4 加密管理政策：機密等級為「機密」之資訊資料類資訊資產，於進行傳輸或儲存時，皆應有保護措施。

2.5 金鑰管理政策：使用之金鑰，每年應定期審查金鑰的有效性。金鑰生命週期之管理，應由專人管理。

2.6 螢幕保護與桌面淨空政策

2.6.1 資訊設備應設定電腦螢幕保護時間，無人操作情況下，最長不得超過**10分鐘**，系統畫面應自動進入密碼保護狀態。

2.6.2 人員離開座位時，應將桌面整理淨空，機密等級為「機密」之資訊資料類資訊資產，應採取保護措施。

7

7

資訊安全政策

2.7 備份政策：可用性價值為「高」之資訊資料類資訊資產，應擬定備份計畫，並依據計畫進行備份作業、保存及還原測試。

2.8 資訊傳輸政策：資訊資料類之資訊資產，若機密等級為「機密」應設定保護機制；與外部團體間之資訊傳輸，應事前申請並經資訊保有之權責單位主管核准後，方能傳輸。與外部團體間如為傳輸機密等級為「機密」之資訊資料類資訊資產，傳輸過程應有安全之保護機制。

2.9 安全開發政策：本公司無自行開發需求，皆採購市面上之應用程式或系統。

2.10 委外廠商資訊安全管理政策：應與委外廠商建立專案之資訊安全管理需求，並在委外本廠商履行合約義務過程中，實施必要之管理與稽核活動，確保委外廠商提供之服務與產品，符合專案之資訊安全管理需求。

8

8

資訊安全政策

■**資訊安全目標**

1. 本公司之**資訊安全管理目標**為：
   - 1.1 保護本公司業務活動資訊，避免未經授權的存取。
   - 1.2 保護本公司業務活動資訊，避免未經授權的修改，確保其正確完整。
   - 1.3 建立跨部門之資訊安全組織，制訂、推動、實施及評估改進資訊安全管理事項，確保本公司具備可供業務持續運作之資訊環境。
   - 1.4 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
   - 1.5 執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。
   - 1.6 實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。
   - 1.7 本公司之業務活動執行須符合相關法令或法規之要求。

9

9

資訊安全政策

■**資訊安全目標**

2. 為達成本公司資訊安全管理目標，參考ISO/IEC 27001國際標準要求，建立資訊安全管理制度，對資訊安全管理制度實施範圍內之資訊資產採取適當保護措施，以維持資訊資產之機密性、完整性與可用性，提供客戶安全之資訊服務並滿足其需求。

3. 資訊安全工作小組應每年或當發生重大變更時檢視與評估資訊安全管理目標，若需要調整資訊安全管理目標，應提請資訊安全委員會核准。

10

10

資訊安全政策

■**資訊安全管理制度制訂與實施**

1. 資訊安全執行小組（個人資料保護推動執行小組）應每年或當發生重大變更時，應依據「**YAN-ISMS-02-15資訊安全全景與關注方規劃程序書**」之要求，執行組織全景分析作業。
2. 資訊安全執行小組（個人資料保護推動執行小組）應依據全景分析結果及資訊安全管理政策與目標之要求，制訂與維護資訊安全管理制度、推動與管理資訊安全管理制度之實施、監控與評估資訊安全管理制度之績效及持續改善資訊安全管理制度。
3. 本公司資訊安全管理制度要求，係以滿足組織全景分析與資訊安全風險評鑑之結果所訂定，資訊安全執行小組（個人資料保護推動執行小組）應遵循相關政策及作業規定，督導本公司同仁依規定實施各項作業流程要求。

■**審查與修訂「適用性聲明書」**

資訊安全執行小組（個人資料保護推動執行小組）應每年完成風險評鑑作業後或當發生重大變更時，審查與修訂「**YAN-ISMS-01-02適用性聲明書**」，對於適用及不適用之控制措施應說明其原因，並提請資訊安全管理委員會審查核准。

11

11

資訊安全目標宣導

■依據：YAN-ISMS-02-01資訊安全暨隱私保護組織程序書

■版次：2.2

1. 資訊安全執行小組（個人資料保護推動執行小組）應每年定期評估本公司資訊安全管理制度之實施績效和效果。
2. 資訊安全執行小組（個人資料保護推動執行小組）應對所蒐集資訊安全管理績效資料，依據規劃期程進行監控與分析，並製作「**YAN-ISMS-04-03 ISMS_PIMS 有效性量測表**」。

12

12

隱私保護政策

■文件編號：YAN-PIMS-01-01 隱私保護政策

■版次：1.1

■目的

延宇資訊股份有限公司（以下簡稱本公司）為強化個人隱私資料管理，確保所屬之個資資產的機密性、完整性及可用性，以提供本公司之個人資料管理業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。。

13

13

隱私保護政策

■適用範圍：

- 本公司所有處理個人資料單位與人員。

■定義：

1. 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
2. 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
3. 蒐集：指以任何方式取得個人資料。
4. 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
5. 利用：指將蒐集之個人資料為處理以外之使用。
6. 個資資產：係指為凡存有個資資料的文件、檔案、媒體均屬之。

14

14

隱私保護政策

■組織角色

- 本公司處理個人資料之角色為 PII 控制者及 PII處理者

■政策內容

1. 本公司遵循「個人資料保護法」之規定，履行相關法定告知義務。
2. 建立符合國際標準的個人資料管理系統（以下簡稱PIMS），使隱私保護政策得以落實。
3. 應提供明確之管道讓個人資料當事人知悉其個人資訊將如何被使用及被誰使用的清楚資訊。
4. 本公司只會基於合法的特定目的，在確實必要的範圍內，誠信、合法、相關且適當之方式最小化地蒐集、處理、利用個人資料，嚴禁一切非法或非屬業務目的之行為。
5. 已蒐集之個人資料僅會作適當且相關之處理，並依法或於合法之特定目的下進行妥善保存及刪除。
6. 就本公司所持有之個人資料建立類別清單，並維持個人資料的正確性及適時進行更新。
7. 尊重當事人對其個人資料所能行使之權利，包含查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用及請求刪除等。

15

15

隱私保護政策

8. 本公司個人資料不進行國際傳輸。
9. 本公司將以合於時代之技術措施及管理制度，全力保護當事人之個人資料，維持本公司持有之個人資料的安全，以避免當事人個人資料被竊取、洩漏、竄改或受到其他侵害。
10. 鑑別內外部利害關係者及其參與個人資料管理制度治理與運作程度，並於個人資料管理制度運行中，明確界定同仁之義務與責任。
11. 含有個人資料的檔案應該被限制儲存在有適當的安全保護與品質控管的集中管理系統當中，所有非集中管理的資料庫都應該被鑑別出來。
12. 若發生個人資料外洩事件，本公司承諾於查明事件後，以適當方式通知當事人並進行適當之處理。
13. 如有個資委外需求時，所有委外合約都應有正式的書面文件，每份委外合約都應涵蓋個人資料保護精神，以確保委外廠商所蒐集、處理、與利用的個人資料受到與本公司要求相同程度的保護。

16

16

隱私保護政策

■**政策目標**

依據隱私保護政策擬定其目標如下：

1. 辦理個人資料保護教育訓練，推廣人員保護之意識與強化其對相關責任之認知。
2. 保護本公司業務流程之個人資料，避免未經授權的存取與竄改，確保其機密性及完整性。
3. 確保本公司業務流程之個人資料蒐集處理利用，符合法令法規及相關契約之要求。
4. 維護個人資料之當事人權利之完整性與有效性。

■**目標管理**

➢ 「資訊安全執行小組（個人資料保護推動執行小組）」應於管理審查中，針對個人資料管理目標有效性量測結果，向「資訊安全暨隱私保護委員會」進行報告。

17

17

隱私保護政策

■**責任**

1.本公司的「資訊安全暨隱私保護委員會」建立及審查此政策。

2.「資訊安全執行小組（個人資料保護推動執行小組）」透過適當的標準和程序以實施此政策。。

3.所有人員和委外服務廠商均須依照相關安全管理程序以維護隱私政策。

4.所有人員有責任報告個人資料安全事件和任何已鑑別出之弱點。

5.任何危及個人資料安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司之相關規定進行懲處。

■**審查**

本政策應至少每年審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本公司永續運作及個人資料安全實務作業能力。

■**實施**

1.「隱私保護政策」配合管理審查會議進行「隱私保護政策」審核。

2. 本政策經「資訊安全暨隱私保護委員會」進行審核後實施，修訂時亦同。

18

18

人員資訊安全暨隱私資料安全守則

■文件編號：YAN-ISMS-04-17人員資訊安全暨隱私資料安全守則

■版次：2.0

■目的

➢ 為落實延宇資訊股份有限公司（以下簡稱本公司）資訊安全暨隱私保護作業，維護資訊及處理設備之機密性、完整性及可用性，特訂定此守則。

19

19

人員資訊安全暨隱私資料安全守則

■**依據：YAN-ISMS-04-17人員資訊安全暨隱私資料安全守則**

■**範圍：本守則適用於正職人員與臨時人員**

1. 電腦應設定密碼確實保密。
2. 電腦應設定螢幕保護程式（10分鐘）並設定密碼保護。
3. 電腦之作業系統漏洞應即時更新修補。
4. 電腦應安裝公司選用之防毒軟體並即時更新病毒碼。
5. 應定期將重要資料備份存放。

■**使用通行密碼應注意下列要點：**

1.應保護通行密碼，維持通行密碼的機密性

1.1資訊系統之管理者應至少每3個月更換通行密碼一次，並禁止重複使用相同的密碼。

1.2系統一般使用者應至少每3個月更換通行密碼一次，並禁止重複使用相同的密碼。

2. 應避免將通行密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。

20

20

人員資訊安全暨隱私資料安全守則

3. 當有跡象顯示系統及通行密碼可能遭破解時，應立即更改密碼。
4. 通行密碼的長度最少應有8位長度以上，且需有數字、特殊符號、英文共同組成之密碼。
5. 密碼設置原則，應儘量避免使用易猜測或公開資訊為設定：
   - 個人姓名、出生年月日、身分證字號。
   - 公司或單位名稱識別代碼或是其他相關事項。
   - 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。
   - 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。
   - 電話號碼或英文或是其他外文字典的字彙。
   - 專有名詞或空白。
6. 除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。
7. 除公司核定同意外，任何人不得在任何公開的新聞群組、論壇、或公布欄中透露任何有關本公司資訊細節。
8. 在丟棄任何曾經儲存本公司資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀或實體破壞至無法解讀之程度。

21

21

人員資訊安全暨隱私資料安全守則

9. 限閱等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。
10. 機密文件或合約，應妥善保存；若為電子檔案應考慮設定保護密碼或採用其他保密措施。
11. 開啟來路不明之電子郵件及其附件時應謹慎小心，以防電腦中毒。
12. 當有跡象顯示系統可能中毒時，應儘速通知相關人員。
13. 禁止濫用系統及網路資源，複製與下載非法軟體。
14. 電腦軟體版權之使用與管理：
    14.1 經由公司採購流程所取得之合法軟體，始可於公司內部使用。
    14.2 本公司所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。
    14.3 除公務使用外及未經公司部主管級以上主管同意，不可複製公司內部之軟體、文件資料至公司以外之場所使用或販賣。
    14.4 軟體之重製應以符合該軟體授權合約書之條約內容為基準，且需單位主管同意；不得為任何合約書規定以外的拷貝、複製行為。

22

22

人員資訊安全暨隱私資料安全守則

14.5 不可複製非經公司採購的非法軟體（含共享軟體）到公司安裝使用。若為測試軟體應經單位主管同意始可使用。超過測試（試用）期間應予移除。
14.6 應確定電腦內軟體具有合法版權後再行使用，以維護個人的權益；如發現公司內有任何不法使用之軟體及相關文件，應即告知管理單位，並由資訊人員協助處理。
14.7 任何私人可攜式媒體（NB、隨身碟、SD卡..）上的程式或資料，造成公司內部電腦設備有所損害或中毒或破壞電腦資料，則需負擔起賠償責任。
14.8 個人因職務所獲得公司內部系統的帳號、密碼（如進防火牆、伺服器、銷存系統、E-mail帳號...等）皆屬公司資產應妥善保管，不得公開（或與其他人共用）。
14.9 不試圖入侵（hacking）公司任何電腦系統（個人有意或無意使用他人帳號、密碼亦屬入侵行為）。

23

23

人員資訊安全暨隱私資料安全守則

14.10 本公司人員若有安裝軟體需求時，需填寫「設備異動申請單」，經權責主管以上核准後，始得執行安裝。
15. 應遵守「個人資料保護法」規範，保護個人資料使用之合法性、正確性及機密性。
16. 保密協定：
    本公司人員應填具「保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密（包含客戶提供之個資），非經主管授權不得對外透露或加以濫用。
17. 本公司員工若未遵守上述規定或資訊安全政策、隱私保護政策及程序者，得呈報管理部，依本公司相關懲戒程序處置違紀人員。

24

24

新進人員個資保護宣導須知

■文件編號：YAN-PIMS-04-09 新進人員個資保護宣導須知

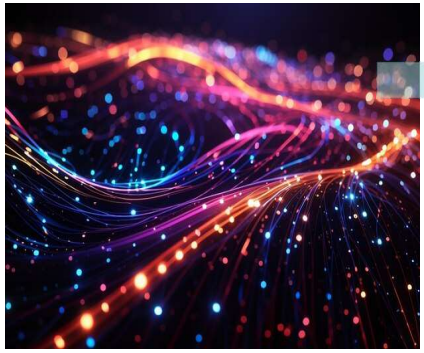
■版次：1.1

■**個資保護日常作業注意事項**

1. 為確保本公司所持有之個人資料皆被適法的蒐集、處理及利用，同仁於日常工作中，應提升個人資料保護意識，並將本公司所訂定之個人資料保護管理措施，落實於個人日常作業流程之中。（例如，離開座位時，應關機或啟動電腦螢幕保護程式；含有個人資料之紙本，應收妥置於抽屜或櫃子...等等。）
2. 遇有個人資料侵害事件發生，應立即通報個資委員代表或總經理。
3. 違反「個人資料保護法」可能導致嚴重之刑事、民事及行政責任，請同仁務必留意。
4. 本公司個人資料保護專責單位為個人資料保護推動執行小組，如有「個人資料保護」問題，敬請與個人資料保護推動執行小組聯繫洽詢。

25

25



二、AI 時代下的法規趨勢與資訊安全守則

- 法規與政策新篇章
- 2026 全球資安大趨勢
- Agentic AI 代理式人工智慧的風險
- 資安暨個資防範實務

26

26

法規與政策新篇章



27

27

法規與政策新篇章
全球AI治理正由「原則」走向「強制監管」

➢ **價值原則**

2019年 **經濟合作暨發展組織(OECD)：通過「人工智慧建議書」提出基本價值原則。**

歐盟(EU)：發布「可信賴人工智慧倫理準則」。

原則 2019

法規 2021

法規 2022

治理 2023

治理 2024

28

28

法規與政策新篇章

全球AI治理正由「原則」走向「強制監管」

➢ 法規制度

2021年 歐盟(EU)：提出「人工智慧法」草案 (AI Act)。

2022年 美國：發布「AI 權利法案藍圖」。

加拿大：提出「人工智慧資料法草案」(AIDA)。



29

29

法規與政策新篇章

全球AI治理正由「原則」走向「強制監管」

➢ 法規治理

2023年 美國：發布「發展與使用安全且可信任的 AI 行政命令」。

2024年 歐盟(EU)：「人工智慧法」(AI Act) 正式通過審議。

韓國：通過「人工智慧發展及建立信賴基盤之基本法」。

英國：發布「生成式人工智慧治理框架」。

新加坡：發布「生成式 AI 治理架構」。



30

30

法規與政策新篇章

AI 治理雙軸並進

- 中華民國於2026年115年1月14日發布「人工智慧基本法」。
- 風險分類框架：數發部將 AI 應用納入風險管理，針對民生、金融、醫療、教育等領域優先審核，組織在規劃資訊安全系統時需具備「風險分級」意識。

七大原則

人工智慧基本法第四條：



31

31

法規與政策新篇章

- 生成式內容標示指引
- 來源透明化：針對 AI 生成影像與深偽內容（Deepfake），政府將推動標示制度。
- 資安法修法重點與委外管理
- 擴大納管：資安法將原本的行政命令提升至法律層級，強化對人工智慧產品或系統高風險產品的管制。
- 委外資安要求：明確要求委外廠商建立完善管理機制或通過第三方驗證，確保維運安全。

32

32

2026 全球資安大趨勢

全球地緣政治與監管環境快速變化：
各國監管部門強化企業高階管理者在資安事件中的責任要求。

代理式AI 風險(Agentic AI) ：
自動化工具與低程式碼工具可能產生未受管理的漏洞。以及身分識別與存取管理對傳統架構帶來新挑戰。

韌性重於防禦：
當攻擊不可避，企業更強調系統受損後的「快速恢復能力」。

- **量子運算加密風險**
- **AI驅動的安全營運中心**
- **生成式AI的普及**

33

33

影片觀賞：中製生成式AI藏資安危機！

34

34

2026 全球資安大趨勢
風險情境



情境1：AI客服

訓練資料含客戶對話
→ 個資外洩風險

資料層防護：
去識別化，最小化蒐集。



情境2：影像辨識

人臉資料未合法取得
→ 違反個資法

應用層防護：
身分驗證，操作紀錄。



情境3：生成文件

輸入敏感資料（如合約）→ 被模型記憶或外洩

模型層防護：
輸入過濾，防資料洩露。

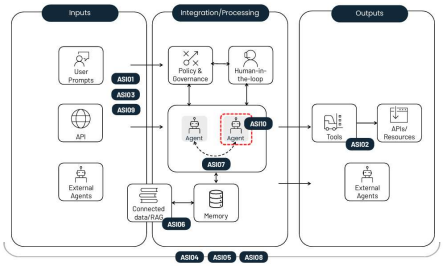
35

35

Agentic AI 代理式人工智慧的風險

Agentic Top 10 At A Glance

ASI01：代理目標劫持（Agent Goal Hijack）
ASI02：工具濫用與調用（Tool Misuse and Exploitation）
ASI03：身分與權限濫用（Identity and Privilege Abuse）
ASI04：代理式供應鏈漏洞（Agentic Supply Chain Vulnerabilities）
ASI05：非預期程式碼執行RCE（Unexpected Code Execution RCE）
ASI06：記憶體與上下文毒化（Memory & Context Poisoning）
ASI07：不安全的代理間通訊（Insecure Inter-Agent Communication）
ASI08：連鎖故障（Cascading Failures）
ASI09：人機信任利用（Human-Agent Trust Exploitation）
ASI10：失控代理（Rogue Agents）



36

36

Agentic AI 代理式人工智慧的風險

- ASI01：Agent Goal Hijack - 代理目標劫持
  在代理式架構下，指令與資料混雜於同一自然語言脈絡，代理無法可靠地區分合法指令與攻擊者控制的內容。
- ASI02：Tool Misuse and Exploitation - 工具濫用與調用
  人員使用AI輔助開發模式，結果整個檔案被rm -rf指令刪除，這正是「給了合法工具，卻被以不安全或非預期方式執行」的典型。
- ASI04：Agentic Supply Chain Vulnerabilities - 代理式供應鏈漏洞
  若惡意套件偽裝成合法的MCP服務，一旦AI Agent調用其功能發送郵件，該套件便可能暗中將郵件密件副本傳給外部第三方，導致敏感資訊外洩。
- ASI07：Insecure Inter-Agent Communication - 不安全的代理間通訊
  自主代理會透過API、訊息匯流排、共用記憶體以保持持續通訊與協作，在身分驗證、完整性、機密性或授權上的控制較為薄弱，攻擊者得以攔截、竄改、冒充或阻斷訊息。

37

37

影片觀賞：AI代理人「龍蝦」爆紅



38

38

資安暨個資防範實務

□針對代理式 AI 的開發防護

- ✓權限最小化： 給予 AI Agent 的 API 權限應受嚴格限制。
- ✓人機協作審核： 在 AI 執行關鍵動作前（如刪除資料），必須經過人類確認（Human-in-the-loop）。

□個資保護新挑戰

- ✓深偽詐騙防範： 員工應警覺任何來自視訊或音訊的異常請求（AI 模擬主管聲音要求匯款或洩漏系統帳密）。
- ✓供應鏈安全： 修法後，作為受託單位，任何個資外洩事件將面臨更嚴峻的行政調查與法律責任。

39

39

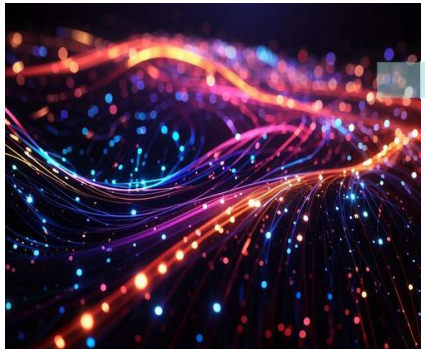
資安暨個資防範實務
情境題



1. 因為方便，把資料丟給AI整理。
   不輸入敏感資料，AI≠安全環境。
2. 為了趕時限，權限先全開再說。
   權限以「最小權限原則」基準執行。
3. 為了測試，用真實個資。
   不隨意交出個人資料。

40

40



三、近期資訊安全暨個資新聞

41

41

Wi-Fi新型漏洞「AirSnitch」

- AirSnitch 的運作方式是，攻擊者只要取得 Wi-Fi 密碼，即可在不破解加密的情況下執行中間人（MitM）攻擊。
- 研究人員測試 11 種主要路由器類型，**幾乎所有測試過的 Wi-Fi 路由器都受影響**，包括使用 WPA2 或 WPA3 的家用與企業網路，**目前尚未確認已有可用的修補程式**。由於此攻擊需要網路存取權（透過 SSID 密碼），因此使用強密碼且不與他人分享的家用使用者，風險低於公共熱點使用者。
- 為降低風險，專家建議使用強且獨特的 Wi-Fi 密碼（含訪客網路密碼），只與可信任對象分享；若路由器支援，啟用用戶端隔離；在公共 Wi-Fi 熱點上使用 VPN 以加密流量；留意韌體更新，因為後續可能釋出修補程式；並避免任意分享密碼。



資料來源：資安快報 https://infosecu.technews.tw/2026/03/05/airsnitch-mitm/

42

42

心理健康App曝上千漏洞，治療紀錄恐成高價黑市資料

- 近期研究發現，多款心理健康應用程式存在大量資安漏洞，可能導致使用者的心理狀態、諮商紀錄等高度敏感個資外洩。
- 這些問題多源於**開發過程中資安設計不足**，例如**API防護不當、資料未加密及權限控管鬆散**，使駭客有機會取得並濫用相關資料。
- 由於心理健康資訊具有高度私密性，其在地下市場亦具相當價值，一旦外洩，可能造成當事人名譽損害甚至被勒索。
- 此事件顯示，即使是非金融或醫療核心系統，只要涉及個資，皆可能成為攻擊目標。整體而言，該案例凸顯企業在系統開發初期即應納入資安與個資保護機制，否則系統上線後即可能面臨重大風險。

資料來源：iThome https://www.ithome.com.tw/news/174014

43

43

影片觀賞：AI假冒公司大老闆 詐團騙匯款



44

44

Windows 記事本爆高危漏洞

- 微軟（Microsoft）近日發布 2026 年 2 月安全更新，修補 58 個漏洞，其中包括 Windows 記事本（Notepad）的高危遠端程式碼執行漏洞（CVE-2026-20841）。該漏洞通用弱點評分系統（CVSS）評分高達 8.8 分，駭客只需誘導使用者開啟含惡意內容檔案並點擊連結，即可完全控制受害者 Windows 系統。
- CVE-2026-20841 漏洞源於 Windows 記事本新增 Markdown 檔案支援功能。微軟在 2025 年為記事本加入 Markdown 渲染功能，讓使用者可直接處理這種輕量級標記語言。然而安全研究員其後發現，**記事本處理 Markdown 超連結時未能正確驗證協議處理器，導致駭客可利用此漏洞執行惡意程式碼**。
- 該漏洞只影響 Microsoft Store 版本現代 Notepad 應用程式，並不影響舊版 Notepad.exe。由於記事本是 Windows 核心元件，幾乎所有現代 Windows 工作站都面臨這個漏洞威脅。
- 微軟已在 2 月 10 日發布 Windows 累積更新中修補此漏洞，並透過 Microsoft Store 推送更新至版本 11.2510 或更高版本。

資料來源：資安快報 https://infosecu.technews.tw/2026/02/23/critical-vulnerability-found-in-windows-notepad/

45

45

OpenSSH存在GSSAPI金鑰交換導致服務中斷漏洞

- Linux常用遠端存取工具OpenSSH存在與GSSAPI（Generic Security Services Application Program Interface）金鑰交換機制相關的漏洞，影響範圍相當大，可能衝擊大量依賴OpenSSH的服務，建議用戶儘速更新。
- 部分Linux發行版在OpenSSH套件中，額外加入的 GSSAPI Key Exchange修補程式存在缺陷，可能在處理GSSAPI相關驗證與連線時造成錯誤，遠端攻擊者只要建立特製連線，就可能觸發錯誤並導致SSH程序終止，導致服務中斷。這項漏洞會影響在OpenSSH中啟用GSSAPI Key Exchange相關功能的系統，解決辦法是安裝Linux修補版本，目前Redhat、Ubuntu與Debian等Linux發行版都已釋出修補程式，

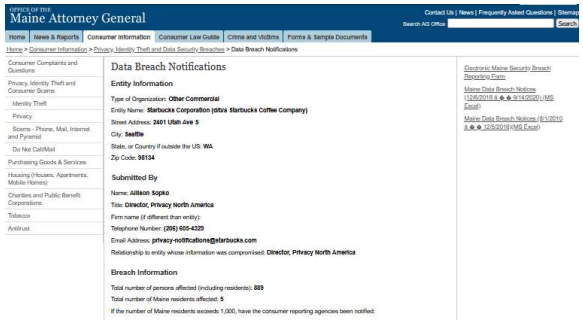


資料來源：iThome https://www.ithome.com.tw/news/174420

46

46

星巴克內部系統遭遇入侵，數百名員工資料外洩



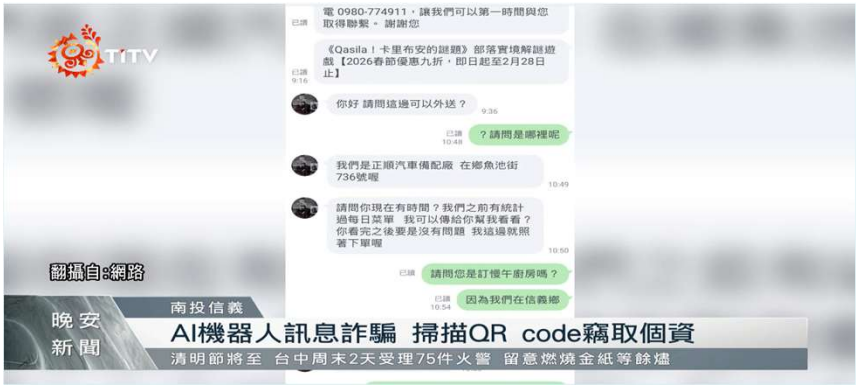
- 攻擊者站入侵國外星巴克內部平臺，造成約 889個員工帳號資訊可能外洩，洩露的資訊包括姓名或其他個人識別碼 。

資料來源：iThome https://www.ithome.com.tw/news/174422

47

47

影片觀賞：疑AI訂餐騙取個資



48

48

Linux核心存在名為「CrackArmor」的資安漏洞

- Linux核心當中的資安防護機制AppArmor存在多項設計缺陷，攻擊者可藉此在本機環境將權限提升至root，對系統安全構成重大威脅。
- 這些漏洞主要屬於混淆代理（Confused Deputy）類型的問題，攻擊者可利用AppArmor在處理權限與資源存取時的邏輯缺陷，繞過既有安全限制，進而取得更高權限。
- 未具特權的本機使用者可透過操控AppArmor相關的偽檔案或安全設定，影響系統對應用程式的存取控制判斷，最終達到權限提升的目的。值得留意的是，這些漏洞不僅影響一般Linux主機，在容器環境中也可能被利用來突破隔離機制，增加橫向移動與系統入侵的風險。

資料來源：iThome https://www.ithome.com.tw/news/174488

49

新字型渲染攻擊手法讓AI助理誤以為網頁無害 (1/2)

- 近期資安公司LayerX揭露一種名為「Poisoned Typeface」的新型攻擊手法，攻擊者僅透過操控網頁中的自訂字型與CSS樣式，即可讓AI助理誤判內容安全性，進而誘導使用者執行惡意指令。
- 此攻擊的核心在於利用「網頁實際顯示內容」與「AI解析的HTML內容」之間的落差。AI通常僅分析DOM文字內容，但經過字型與樣式渲染後，使用者實際看到的資訊可能完全不同，使AI誤以為頁面無害，卻讓使用者接收到惡意指令。
- 此類攻擊不需利用瀏覽器漏洞，也不依賴JavaScript或惡意程式，即可影響包括ChatGPT、Claude、Gemini等主流AI助理，顯示AI在內容判讀上仍存在盲點。
- 該事件凸顯，隨著AI逐漸成為使用者判斷資訊可信度的重要工具，一旦其判讀機制遭誤導，可能導致錯誤建議甚至引發資安事件，顯示AI應用在安全與信任層面仍需進一步強化。

資料來源：iThome https://www.ithome.com.tw/news/174481

50

新字型渲染攻擊手法讓AI助理誤以為網頁無害 (2/2)



- 網頁在HTML中看似只是普通的遊戲同人小說，但透過自訂字型映射後，實際顯示內容卻變成引導使用者執行反向shell等惡意操作的指令。

資料來源：iThome https://www.ithome.com.tw/news/174481

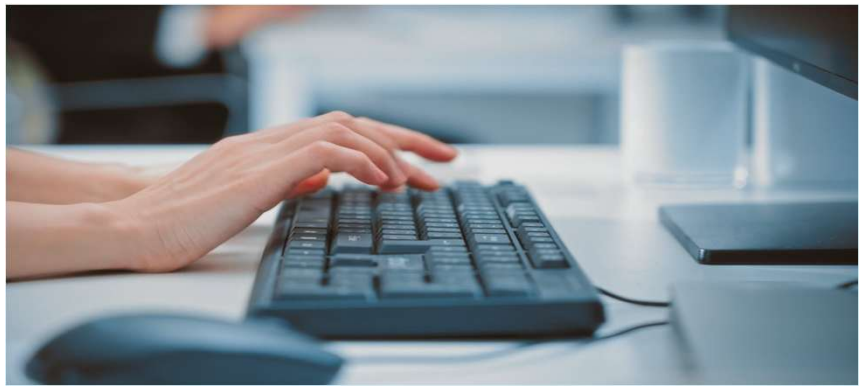
51

影片觀賞：假警察騙個資逼真



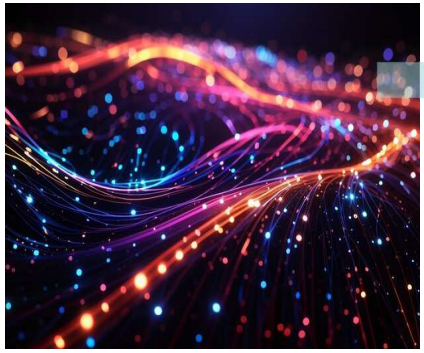
52

影片觀賞：反詐騙宣導_盜用LINE帳號



53

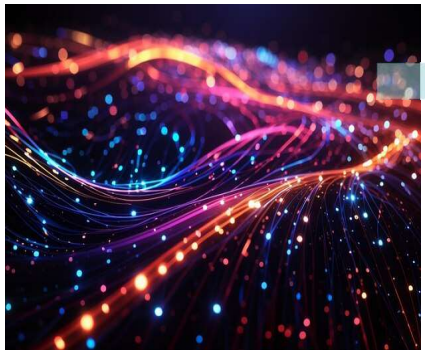
53



五、Q & A 時間

54

54



六、隨堂測驗

55

55



56

56