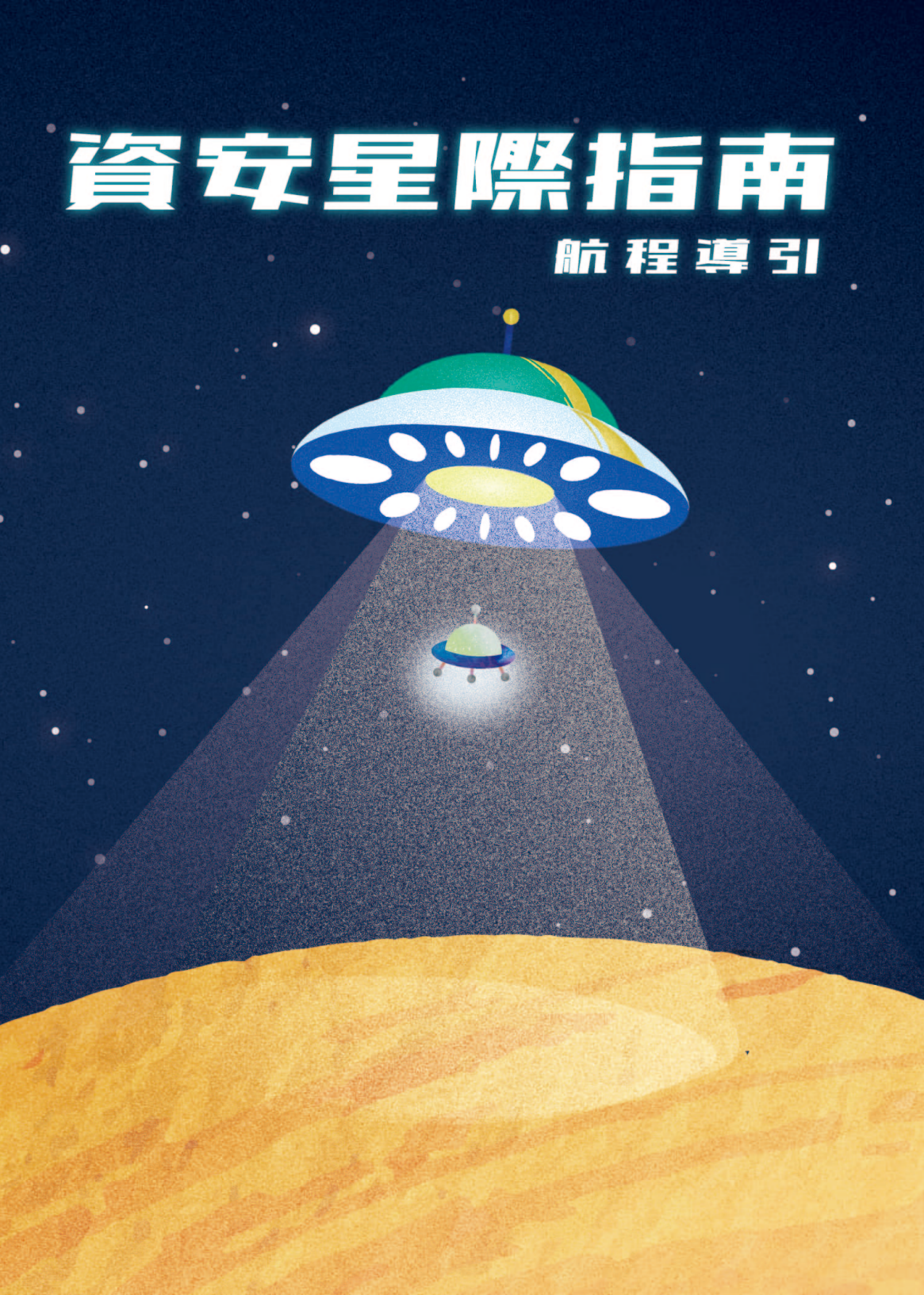
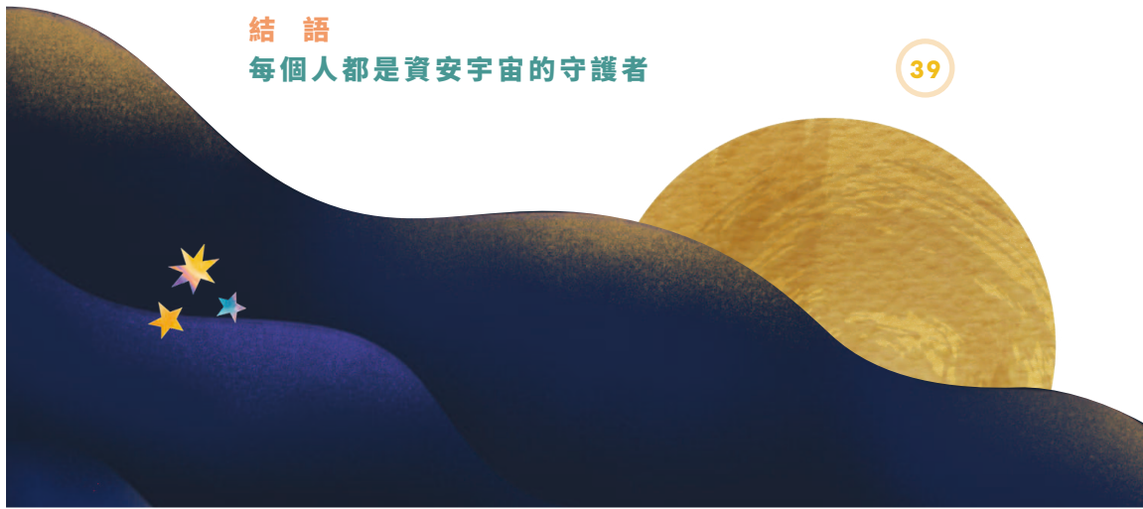
資安星際指南

航程導引





整裝待發
啟動您的資安航程

親愛的中小企業與非營利組織夥伴們，我是椒魚，您的資安專屬領航員！歡迎登上這趟《資安星際指南》的旅程！

這是整套《資安星際指南》的起點冊，幫助您快速了解指南手冊全系列的架構與使用方式。

椒魚

性格溫和的台灣山椒魚，是源自冰河時代的孑遺物種，祖先累積了豐富的經驗和知識，指引星際旅人。

《資安星際指南》是為您量身打造的資安入門指引，協助您在廣闊複雜的資安宇宙裡，找到清楚的起點。

當您面對陌生的資安術語、看似艱澀複雜的步驟時，腦中可能會浮現：「我看得懂嗎？資安跟我真的有關嗎？」
—— **別擔心！有我陪您，不用害怕迷路。**

在接下來的航程中，我會用最簡單的文字、最貼近日常的故事，帶您認識每個星球上真實發生的資安挑戰。我們將遇見努力顧店的小雉、剛入職場的大山、熱血的龜龜，以及聰明冷靜的海豬仔。

他們的故事，正是多數組織每天都在上演的資安現場。

我的任務，就是成為您的導航系統，幫助您快速掌握這套手冊的精髓，精準找到適合的解方。

準備好了嗎？讓我們一同啟航，探索資安宇宙的奧秘吧！

國家資通安全研究院
National Institute of Cyber Security

Chapter 1
開啟航行指南——手冊使用方式介紹

本系列手冊採獨立編撰，讀者可依需求選讀各冊內容。但如果您想循序漸進，建議您先從**《資安星際指南：資安基礎概論》**開始。

基礎概論是這套系列手冊的根基，帶您快速認識資安的基本觀念、常見威脅，以及中小企業與非營利組織最容易遭遇的風險。

《資安基礎概論》

《資通系統安心委外》

藉由常見資安情境打好基礎，後續在閱讀其他本手冊時，就能把情境和實務需求連結在一起。

接下來，您可以依照自己的需求，選讀以下三本手冊：

《資通系統安心委外》、《網路安全輕鬆學》、《資安制度全攻略》

《網路安全輕鬆學》

《資安制度全攻略》

這三冊內容彼此獨立，沒有既定的閱讀順序。
建議手冊內文的閱讀方式如下：

① 讀故事 → 進入情境

每章開頭都有**不同星球住民的真實冒險故事**，像是「信箱突然收到異常登入通知」或「該怎麼擬訂資安制度」。您可以將自己的角色代入到故事中，想像如果是您，面對同樣的狀況，會怎麼做？

💡 這些故事來自中小企業與非營利組織常見的情境，讓您更快抓到問題核心。

② 看知識 → 拆解觀念

在故事之後，會出現**資安知識重點整理**。把艱澀的制度、專有名詞，用最淺白的語言講解。

💡 書中的「🚩 小提醒」提示您最容易忽略的環節。

③ 學方法 → 馬上可用

章節裡都有**清單、範例、操作流程、對照表**。不只是理論，而是提供清楚的 SOP，可以直接套用到組織工作中。

💡 每個章節結尾的「下一章導引」能幫助您把觀念串聯起來，逐步建立完整流程。

④ 自我檢查 →筆記本

每章最後，都附有星球住民的**筆記本**（自我檢查清單），方便您查核該章節的重點、並對照自身狀況。

💡 跟著問題一一檢視，就能清楚知道「我們做到哪裡了」、「還有哪些要補強」。

⑤ 延伸閱讀 → 持續進修

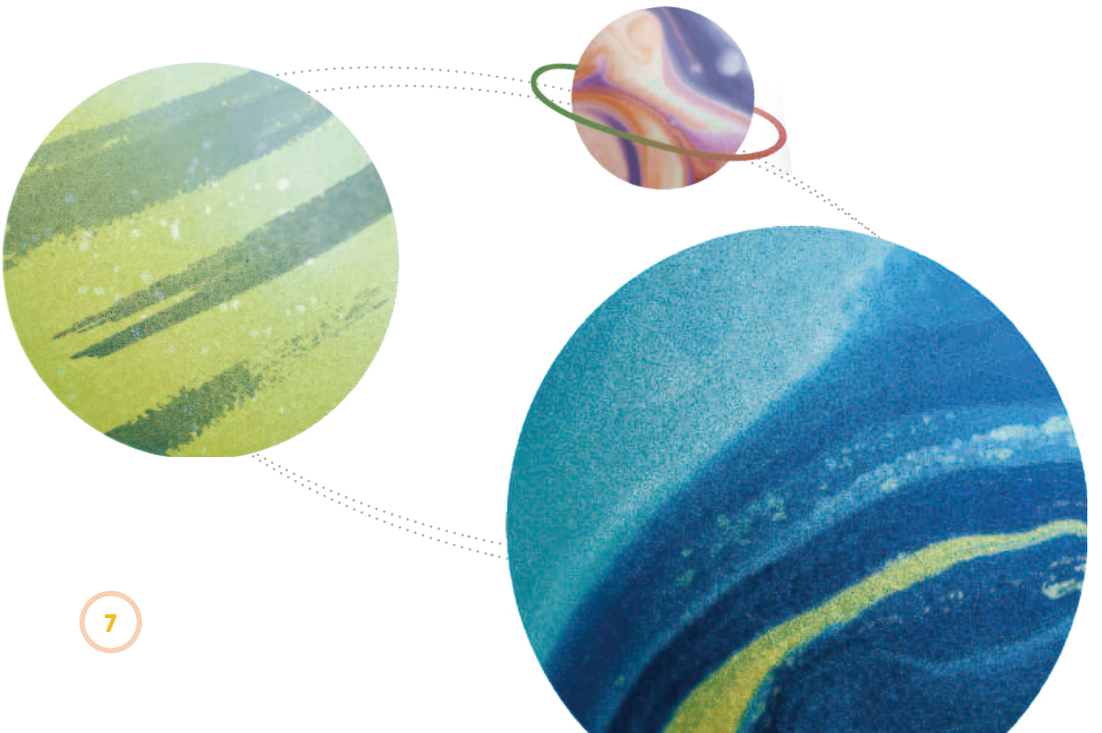
章節中若提到專有名詞，會在單元後放上**延伸閱讀與補充資源**，像是 SLA（服務等級協議）、IoT 裝置風險、相關政府公開資源等。

💡 當您要深入研究，或準備和廠商、團隊討論時，這些就是最可靠的後盾。

Chapter 2
探索資安地圖 —— 四大主題航線任務

這套手冊共有四大主題，分別從「資安概論、系統委外、網路安全、制度管理」四個面向，帶您循序漸進地認識並實踐資通安全。

內容穿插星球住民們的故事，讓抽象的資安概念轉化為貼近具體實務現場的情境。無論您是中小企業的管理者、非營利組織的行政人員，或是剛接觸資安的新手，都能從這四冊中找到可立即應用的實務指引。



主題一

《資安星際指南：資安基礎概論》

從眞實案例出發，理解資安基礎概論

資安不只是資訊人員的責任，而是需要管理層與每一位員工共同面對的課題，只要人人保持警覺，對資安的全貌有更清楚的輪廓，知道該從哪裡開始做防護，就能大幅降低風險。

★在這本手冊中，您可以學習以下內容

① 資安威脅

從眞實案例出發，了解釣魚郵件如何導致郵件系統被入侵，帳號資料外洩、捐款資料外洩如何讓公益團體失去信任等，認識近年的**四大資安威脅趨勢**。

② 資安三要素

介紹資安的基礎原則，**機密性、完整性和可用性**，簡稱「CIA三要素」。所有資安措施的設計與實施，都應以此為依歸。

③ 多層面防護

資安涵蓋八大層面，除了常聽到的資料安全，也包含社交工程、行動裝置、通訊軟體安全、網路服務、實體安全、委外與人力資源安全等。我們將這些層面的風險與威脅，透過實際案例，讓您更清楚如何預防相關危機。

主題二

《資安星際指南：資通系統安心委外》

如何在將資訊系統委給外部廠商的過程中確保資料與系統的安全性

這一冊將陪您走過資通系統委外的五個關鍵階段，幫助您在開發前釐清風險、簽約時守住條款、驗收時確保品質，避免「先做出來再說」而忽略資通安全。

星球故事 —— 甜點星球上的小雉與阿虎

隨著餅乾店生意蒸蒸日上，老闆決定要進軍網路市場，請小雉找廠商委外打造一個線上訂購系統。小雉滿心以為這只是單純的「把商品放到網站上」的任務，卻沒想到，委外背後隱藏的挑戰與風險，比他想像的還要複雜許多。幸好有阿虎在旁相助，這趟委外之旅才不至於變成一場災難。

在這本手冊中，您可以學習以下內容

① 尋找廠商前

釐清自身需求並了解組織可能面臨的**潛在風險**。

② 洽談初期

掌握合約中必須納入的**關鍵資安條款**，例如：資料保護、資安事件通報機制。

③ 系統開發中

提醒廠商需特別注意的**資安開發重點**，並確保程式碼本身是安全的。

④ 系統完成

在**正式上線前徹底檢查**系統是否符合預期的安全標準。

⑤ 系統正式啟用後

了解如何與廠商合作，**持續進行資安維護**。

主題三《資安星際指南：網路安全輕鬆學》

如何在資源有限的情況，守護組織的網路安全底線

這一冊將從常見的資安威脅開始，陪您逐步建立起實用的防護策略，讓資安成為每位成員的日常習慣。

星球故事 —— 星際環境保育星球上的大山與老鼻

大山滿心以為只要「顧好電腦、插好網路線」就可以完成任務，直到聽聞某公司網站被駭、顧客資料外洩，他才發現，這份任務比想像中棘手得多。從無線網路、帳號管理到防範釣魚信，每一環都可能是駭客的突破口。幸好有老鼻在旁，帶著他一步步拆解危機、學會守護組織的祕訣。

在這本手冊中，您可以學習以下內容

① 網路與防火牆

經由修改路由器的**預設密碼**、開啟防火牆，設定內部網路區隔，避免某台設備被攻陷，病毒沿網路擴散的風險。

② 設備安全

提醒看起來無害的**物聯網設備**，如攝影機、印表機等，因為**使用預設密碼或未更新韌體**而成為駭客的入口。

③ 無線網路安全

公共 Wi-Fi 潛藏風險、**VPN** 如何為資料傳輸加密、較不易破解的 **Wi-Fi 加密協定**。

④ 帳號與郵件安全

拆解**社交工程**的常見手法，透過**多因子驗證、設定強密碼**，以及**避免帳號共用**來做好防護。

主題四《資安星際指南：資安制度全攻略》

如何將「資安意識」變成組織內穩定運作的「流程與制度」

這一冊將從零開始，一步一步建立資安制度，讓制度成為走向穩定與安全的日常，而非瑣碎複雜的負擔。

星球故事—— 海湧觀光星球上的海豬仔與龜龜

海湧觀光管理局的官方網站頻頻遭到惡意攻擊，資安制度的漏洞逐漸浮現。海豬仔與龜龜肩負起強化制度的任務，從資產盤點到風險評估，一步步打造出守護星球的資安防線。

在這本手冊中，您可以學習以下內容

① 資安政策與願景建立

以 **ISMS 管理框架**與 **PDCA 循環**為核心，從願景、政策、目標、制度四個層次出發，建立清楚的方向與實作規範。

② 資訊資產盤點與價值評估

文件、系統、硬體、人員等等，全面識別資訊資產，透過**機密性、完整性、可用性與法遵性**四項指標計算資產價值，為風險評鑑奠定基礎。

③ 風險評鑑與制度落實

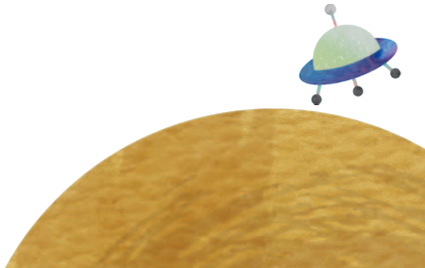
結合資產價值、威脅等級、脆弱性等級三項因素計算風險值，採取**降低、避免、轉移、接受**等策略，並以程序書落實在日常作業中。

④ 稽核、演練與營運持續計畫：

透過**內部稽核、記錄追蹤與桌上推演**，驗證制度是否有效；利用 **BCP** 模擬災難情境，確保在斷網或系統故障時仍能維持運作。

各冊關鍵主題綜覽

	電子郵件	帳號安全	Wi-Fi	IoT 裝置	資料備份	風險評估	委外管理	資安稽核	資安應變	資安制度
 資安基礎概論	釣魚信件 社交工程基礎概念	基本注意事項	行動裝置 WiFi 安全		備份 3-2-1	資安風險與威脅案例		委外注意事項	資安事件衝擊面向	中小企業與非營利組織資安推動指引
 資通系統安心委外		測試帳號控管			備份監控 異地備援	委外前風險評估 資安預算納入	需求盤點 合約訂定 驗收到維運		建立應變流程	
 網路安全輕鬆學	釣魚信件辨識與應對	雙因子多因子驗證	公共 WiFi 假冒熱點的風險	IoT 設定 原廠密碼風險		常見資安風險 資料價值 風險程度				
 資安制度全攻略	電子郵件處理與通報	帳號啟用與停用規範			單一備份的風險 多重備援的重要性	風險矩陣評估與排序		內部稽核 事件演練 成效追蹤	資安事件通報與應變演練	PDCA 循環 程序書撰寫與落實



Chapter 3
星際問答集——
解鎖您最關心的資安疑問

現在請跟隨椒魚我，啟程巡遊資安宇宙，帶您逐一走訪各星球，揭開他們在資安防護上最常遇到的疑問，並一一解答。

🚀 **首先第一站，先從資安星際總部開始！**

Q1 為什麼小公司也會成為駭客的目標？

「我們這麼小的公司，為什麼還會成為駭客的目標？」這是大家最常有的疑問。

事實上，駭客看重的是容易得手的程度。資安防護往往不夠完整的小公司，正好成為駭客的下手目標。

他們可能竊取您的**客戶資料、商業資訊**，甚至癱瘓您的**營運流程**。更危險的是，駭客經常把中小企業當作供應鏈裡的薄弱環節，一旦突破，就能一路滲透到更大的合作對象或上游單位，造成嚴重的連鎖傷害。

資安小知識

① 中小企業與非營利組織面臨的常見資安風險

中小企業

- 重要業務系統或網站無法運作、修復困難，或網路長時間斷線，影響客戶合作、訂單處理。
- 機敏資料（如客戶名單、財務、內部郵件、員工資料、智慧財產、專業技術等）外洩或遭竄改，造成金錢、信譽損失，失去客戶信任與商機。
- 遭遇勒索軟體入侵，檔案被鎖定無法存取，必須支付巨額贖金。
- 常在供應鏈中扮演關鍵角色，但資安防護不足，駭客將其視為跳板，藉此滲透到整個供應鏈，造成難以想像的財務與品牌衝擊。

非營利組織

- 捐款人、志工、受助者等個人資料外洩，導致他們接到詐騙電話、釣魚郵件、社交工程攻擊，甚至身份遭盜用。
- 機敏資訊（個案紀錄、救援路徑、人員身分、行動計畫等）遭駭客盜取或曝光，可能危及服務對象、工作者甚至合作機構的安全。
- 組織官網或捐助系統若遭竄改，支付介面可能被植入惡意程式，導致捐助金流遭竊或捐款被引導至不法帳戶，不僅造成資金損失，亦可能使重要公告或資訊被竄改，進而散播錯假內容。

② 資安防護的日常 SOP

面對資安威脅，中小企業和非營利組織的資安防護觀念，應從「滴水不漏」轉為**「降低風險、提升韌性」**。以下是三個您可以立即採取的行動：

建立良好的網路使用習慣

- 定期更新軟體與作業系統，以修補漏洞
- 使用高強度密碼，並開啟多因子驗證（MFA）
- 謹慎開啟不明郵件或連結，以免惡意程式入侵
- 不輕易連接免費公共 Wi-Fi

定期進行員工教育訓練

- 安排定期的資安教育訓練與無預警的社交工程演練
- 透過演練，培養員工辨識詐騙的能力，確保他們面對不同攻擊時能保有警覺性
- 宣導資料管理內訓課程，提升資安意識

隨時做好應變措施

- 制定應變策略，並定期備份重要資料
- 實踐「3-2-1 備份原則」，即至少備份 3 份資料，使用 2 種不同儲存媒體，並將其中 1 份儲存於異地
- 建立偵測與管理資安威脅的機制

詳細說明和更多中小企業與非營利組織面臨的資安風險：請見《星際資安指南：資安基礎概論》

🚀 我們來到了甜點星球，正好碰到小雉與阿虎

Q2 委外廠商會處理資安嗎？合約該怎麼簽？

小雉最近正在評估公司的訂單系統，想找外部廠商幫忙開發。他心想：「專業的事就交給專業的來吧！資安這部分，廠商應該會處理好。」

他把想法跟阿虎分享，阿虎聽了卻搖搖頭，嚴肅地說：「委外開發，不代表資安責任就完全外包。把系統、資料交給外部廠商，等於是讓他們接觸公司的重要資產，如果廠商沒有做好防護，出問題要收拾的還是你們。」

小雉一臉疑惑：「他們不是有專業團隊嗎？我們也不懂技術，怎麼檢查？」

阿虎解釋：「資安外包不能『全權委託』，而是『共同責任』。你與委外廠商的關係，像是共同管理一個重要專案，你負責提出需求、他負責開發執行，但確保專案安全無虞，是雙方的責任。合約，就是雙方共同遵守的準則。」

★ 資安小知識

資通系統委外注意事項

定義權責，說清楚「誰負責」：

在委外合約中，務必明確定義雙方的資安責任。

- **廠商的責任：**確保開發的系統符合資安規範、定期進行弱點掃描、修補漏洞。
- **我方的責任：**提供正確的系統需求、確認資安條款並要求廠商遵守，以及在系統驗收後持續做好日常管理。
- **共同責任：**發生資安事件時的通報與應變，雙方應共同協調與配合。

納入資安條款，把防護「寫進合約」：

合約不該只有價格與功能，資安條款是保護自己的重要防線。建議在合約中加入以下內容：

- **資安要求：**明確要求廠商遵守資安規範，例如不得保留任何預設帳號與密碼。
- **事件通報：**發生資安事件時廠商應立即通報，並協助調查與修復。
- **罰則與賠償：**若因廠商疏失導致資安事件應明訂賠償責任。
- **資料銷毀：**專案結束後，廠商須徹底刪除所有相關資料。

驗收與稽核：

在驗收階段，就應要求廠商提供資安相關的證明文件，如弱點掃描、滲透測試報告、教育訓練證明等。

詳細說明和更多委外安全案例
請見《星際資安指南：資通系統安心委外》

🚀 我們來到星際環境保育星球，觀察大山與老鼻的職場生活

Q3 收到可疑的郵件，該如何判斷與應對？

大山正在整理捐款報表，突然跳出一封標題為「帳號異常，請立即驗證」的郵件。

寄件人看起來像是常用的雲端服務，信裡還附上一個登入連結，指令非常急迫：「若未在 30 分鐘內完成驗證，帳號將被停用。」

大山心裡一驚，正準備點開連結，老鼻剛好路過，看了一眼立刻喝止：「別點！這就是典型的釣魚信，駭客故意用緊急語氣，讓你陷入慌亂。一旦輸入帳號密碼，整個信箱就被盜走了！」

大山嚇得冒冷汗，才明白原來一封看似普通的通知信，竟能隱藏這麼大的陷阱。

⭐ 資安小知識

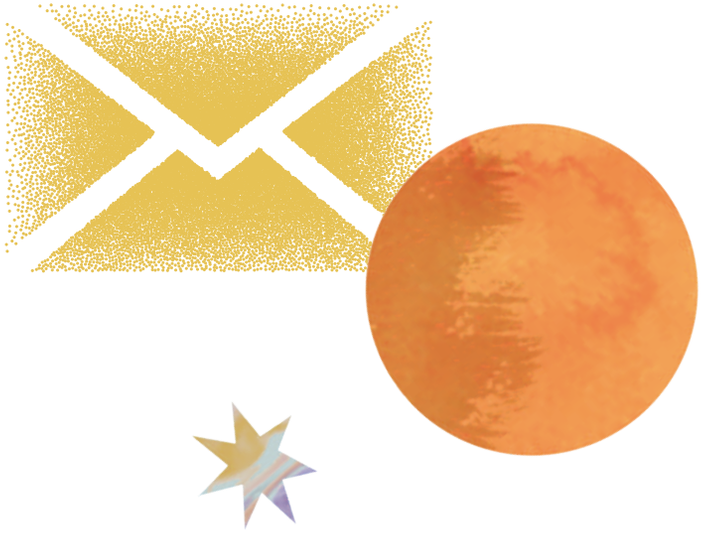
① 電子郵件常見威脅：釣魚信件（Phishing）

這是最常見的電子郵件攻擊。駭客會假冒銀行、郵局、政府機關或常用的雲端服務，製造「緊張感」或「急迫性」，讓人來不及思考就照指示行動。

一旦收件人點擊信中的假連結，就會被引導到偽造的登入頁面，輸入的帳號密碼立即被竊取。

案例

某中小企業的行政人員收到一封「郵局包裹投遞失敗」通知，點擊連結輸入密碼後，信箱被盜，駭客冒用帳號發信給捐款人，造成信任危機。



② 收信與寄信的安全 SOP

電子郵件看似再平常不過，但一個小小的疏忽，就可能讓駭客有機可乘。不用高深的技術，只要養成「收信前檢查、寄信前確認」的習慣，就能降低風險，避免許多意外。

收信前檢查

- **看寄件人：**是否眞的是常見的聯絡對象？信箱網域是否拼錯？（如 .org 被換成 .com）
- **看語氣：**內容是否異常急迫、威脅，或與平常寫信習慣完全不同？
- **看附件：**檢查檔名是否奇怪？有沒有未說明的壓縮檔或執行檔（.exe）？
- **看連結：**滑鼠移到連結上，檢查網址是否眞的是官方網站。

寄信前檢查

- **群發信件請用 BCC：**大量寄送時，把收件人放在「密件副本（BCC）」欄，避免看到彼此的信箱。
- **大量寄送先測試：**先寄一封測試信給自己，確認內容格式正確，避免一次寄錯上百人。
- **敏感資料要加密：**涉及捐款紀錄、會員名單等個資，不應直接夾帶 Excel，至少要加密檔案或使用安全傳輸。
- **簽名檔與說明完整：**正式信件應附上組織名稱、聯絡方式與簽名檔，讓收件人能辨識眞偽。

詳細說明和更多網路安全案例
請見《星際資安指南：網路安全輕鬆學》

Q4

帳號和密碼該怎麼管理，才能避免被盜用或濫用？

大山正在登入組織的募款平台，畫面卻突然跳出一則警示通知：**「有人嘗試從海外登入此帳號。」**

大山愣住了，心裡一陣發毛：「怎麼可能？這組帳號只有我們財務和我在用啊！」

老鼻瞄了一眼，眉頭立刻皺了起來：「你們是不是共用一組帳號？而且密碼是不是很簡單？」

大山支支吾吾地回答：「呃……是的，我們用同一組帳號比較方便啊，密碼就是公司縮寫加 1234。」

老鼻聽完忍不住搖頭：「這樣就等於敞開大門！駭客只要用最基本的猜密碼手法，就能輕鬆闖進去。你以為方便，實際上卻是把募款平台和所有捐款人的資料都曝露在風險裡。」

詳細說明和更多帳號管理資訊
請見《星際資安指南：網路安全輕鬆學》

資安小知識

① 帳號與密碼的常見風險

- **弱密碼：**生日、寵物名、12345678 等，非常容易被破解。
- **一組密碼走天下：**不同平台用同一密碼，只要其中一個外洩，其它帳號也跟著淪陷。
- **共用帳號：**責任不清，離職員工也可能繼續登入，風險極高。
- **未開啟雙因子驗證：**密碼一旦外洩，將難以防止駭客入侵。

② 帳號與密碼管理 SOP

帳號與密碼的管理就像守護組織的鑰匙，只要建立好日常 SOP，就能避免多數風險。

設定密碼時

- 密碼組成建議包含大小寫、數字與符號。
- 避免使用與個人相關的資訊（如生日、電話、寵物名）。
- 不要用常見組合（如 password、abcd1234）。

使用帳號時

- 不要共用帳號：每人都該有自己的帳號，方便追蹤紀錄。
- 重要系統必須開啟**雙因子驗證（2FA）**。
- 建立「權限管理」，讓不同角色只擁有需要的權限。
- 員工離職或職務異動，務必立即停用或調整帳號。

管理密碼時

- 避免隨意抄寫密碼或貼在顯眼處（別貼在辦公室桌面或牆上！）。
- 定期檢查是否有異常登入紀錄，若有可疑活動，立即更換密碼並通報。

Q5 如何管理公司裡的網路設備，確保安全？

大山最近覺得公司的網路變慢了，他在購物平台上下訂了一台效能更好的路由器。

他開心地跟同事說：「我已經換好了路由器，現在大家上網應該會順暢許多！」 老鼻聽了眉頭一皺，問道：「你裝好就直接使用了嗎？有修改過任何設定嗎？」 大山一臉茫然：「設定？不用吧？原廠不是都設定好了嗎？」

老鼻搖搖頭，語重心長地解釋：「為了方便使用者，廠商使用預設的帳號密碼功能，但對駭客來說就像是公開的邀請函。如果沒有修改基本設定，這些設備反而會成為駭客入侵公司的後門。」

資安小知識

① 設備出廠時的預設帳號密碼要更換

原廠帳號密碼多為非常簡單的組合，容易被暴力破解或直接登入。駭客可輕易取得設備管理權限，進而讀取、修改或刪除資料。

② 網路設備管理四步驟

想讓網路設備成為可靠的「資安守門員」，可以從這四個簡單的步驟做起：

第一步：換掉「預設值」

網路設備在出廠時，通常都會有固定的預設帳號和密碼。務必在第一時間變更成複雜且獨特的密碼，並關閉預設的遠端管理功能。

第二步：定期「更新」韌體

韌體就像是網路設備的作業系統。廠商會不斷推出更新來修補安全漏洞，因此定期檢查並更新韌體，是確保設備安全的重要習慣。

第三步：關閉「不必要」的功能

網路設備多餘的功能，例如訪客網路、遠端存取等。如果這些功能沒有必要使用，建議將其關閉。

第四步：規劃「網路區隔」

將公司內部網路與訪客網路、IoT 設備網路分開，即使駭客成功入侵其中一個網路，也無法輕易擴散到整個公司內部。

詳細說明和更多網路安全案例
請見《星際資安指南：網路安全輕鬆學》

最後我們在海湧觀光星球降落，龜龜與海豬仔在制定資安制度

Q6 為什麼「資安制度」需要白紙黑字寫下來？大家心裡有共識和默契不就好了嗎？

海豬仔突然想起一段陳年往事：「以前我在另一家公司時，有位資深技術員突然離職。結果沒人知道主控系統的密碼怎麼重設，整個營運就這樣停擺了 3 個小時。」

「那時我們才意識到，關鍵工作依賴特定人員，且**沒有文件化、系統化及制度化的作業程序，是多麼危險的一件事。**一旦負責的人不在，整個公司就會陷入癱瘓的風險之中。」

龜龜愣了一下，才恍然大悟：「原來，把事情寫下來，才是確保大家都能照著做的關鍵啊！」

海豬仔拍了拍龜龜：「你說的對，除了將作業流程標準化、文件化以外，更重要的是可以依此確認成員是否將規範落實在每天的工作中。」

資安小知識

① 制度的落實：程序書

程序書與作業規範，主要功能在於確保制度可操作與一致性，使組織內不同人員在相同情境下，能依照同一套標準流程執行，降低依賴個人經驗或記憶，並避免作業結果因人而異。程序書的內容通常包含：

- **執行方式**：業務要求與流程
- **責任角色**：由誰負責、誰審核、誰執行
- **時機要求**：何時啟動、多久檢查一次
- **驗證標準**：產出什麼成果或條件才算完成

② 程序書的內容範例

情境	指令流程	負責角色	時間要求
正常運作	系統每日備份 ⇨ 安全日誌記錄 ⇨ 稽核報告	系統管理員 老螺	每日例行 任務
異常警示	偵測異常登入 ⇨ 通報主管 ⇨ 啟動調查程序	資訊人員 魷姐	30 分鐘 以內回應
緊急狀況	資料外洩 ⇨ 啟動應變小組 ⇨ 暫停外部連線	應變指揮官 海豬仔	立即執行

詳細解釋和更多程序書制定說明
請見《星際資安指南：資安制度全攻略》

Q7 哪些東西算是資訊資產？如何做好資產盤點？

龜龜一邊數電腦、一邊拿著紙筆寫寫畫畫，氣喘吁吁地說：

「學長，我已經數完我們辦公室的電腦、印表機和伺服器，這樣資產盤點應該就完成了吧？」

海豬仔搖搖頭：「不只這些喔！資產不只有摸得到的設備，還包含資料、人員、甚至機房環境。任何對組織有價值或需要保護的東西，都算是資產。」

龜龜驚訝地瞪大眼睛：「連研究報告、備份檔案也算？那我們要怎麼整理這些東西呢？」

海豬仔笑著拿出一份表格：「這就是為什麼要做**『資產盤點清冊』**，把所有資產類別、所在位置、負責人、以及它們的重要性分數記錄下來，才算真正的盤點完成。清楚我們擁有哪些資產，就可以進一步判斷每項資產的重要性，並分配資源去保護。」

資安小知識

① 資訊資產類別

資訊資產指的是所有對組織有價值、需要保護的東西。它不一定是「有形」的設備，也包含「無形」的資料與人員。資產盤點的第一步，就是先釐清範圍，弄清楚有哪些東西需要納入管理。以下是常見的資訊資產類別：

- **文件：**公文、報表、紙本紀錄、計畫書
- **軟體：**作業系統、應用程式、自行開發或委外系統
- **硬體：**電腦、伺服器、印表機、監視器
- **通訊設備：**路由器、防火牆、AP、網路線路
- **資料：**個人資料、金流紀錄、研究數據、備份檔案
- **人員：**維護與管理資產的人，以及外包廠商
- **環境：**機房、電力、消防設施

② 資產盤點清冊

每項資產都要有完整記錄，至少包含：

- **資產名稱：**需寫清楚哪個資產，例如「活動網站」、「個人電腦」等
- **資產類別：**屬於文件、硬體、軟體、資料、人員等
- **所在位置：**標示實體位置，或系統中的位置、路徑。如「\\fileserver\2025」、「機房 A 區」
- **權責單位及負責人：**誰要對這個資產負維護管理責任
- **各項指標分數及最終資產價值：**機密性、完整性、可用性及法遵性個別分數及最終評估的資產價值

③ 重要性及價值計算

雖然直覺上覺得「重要的資產」應該一看就知道，但在資產盤點中，光靠感覺並不足夠。由於資源有限，組織必須透過一套標準的方法來計算資產價值，才能判斷哪些需要優先保護。可用四個指標判斷資產的重要性：

- **機密性：**能公開嗎？外洩後會有多大損害？
- **完整性：**被破壞或竄改會造成什麼影響？
- **可用性：**停擺多久可以接受？
- **法遵性：**是否有必須遵循的法規或契約要求？

④ 定期更新盤點

資產清單不是一次就好，組織規模變化、導入新系統、或搬遷機房時，都要重新盤點，才能保持清單的即時性。

詳細解釋和更多資產盤點價值計算說明
請見《星際資安指南：資安制度全攻略》

Q8

出事了還能繼續營運嗎？如何找尋可能的破口？

在例行的資安稽核週，龜龜抱著厚厚一疊報告走進會議室，滿臉得意地說：「看，我們所有平時檢查紀錄都很漂亮！帳號有人管、備份也都有、教育訓練也都有紀錄，是不是代表我們可以安心了？」

海豬仔搖搖頭：「這些紀錄只能證明**平時大家有照做**，但災難發生時，能不能真的活下來，是另一回事。」

說完，他把投影幕打開，出現一行大字：

★ 資安小知識

① 營運持續計畫 (Business Continuity Plan, BCP)

BCP 就是一套「當災難發生時，組織如何維持基本運作」的計畫。**不只檢查平常有沒有做**（備份、權限、訓練），更要**回答災難當下要怎麼做**（誰先通知、幾小時復原、替代方案是什麼）。

② 平時查核與 BCP 差異

檢查面向	平時查核重點	BCP 重點
帳號管理	是否有人共用帳號？ 權限是否合理？	如果管理員突然離職，誰能接手？
資料備份	備份是否完整？ 排程是否有跑？	備份能不能在故障 2 小時內還原？
系統運作	系統是否按時更新？ 是否有備援機制？	系統突然故障時，有沒有異地備援？
教育訓練	員工是否接受過訓練並通過測驗？	員工是否能在模擬事件中正確判定事件並通報？
對外溝通	是否有公告草稿？ 公告發布是否依程序進行？	發生重大事故時，公關能否在 30 分鐘內發布新聞稿或公告於官網？

③ 桌上推演（Tabletop Exercise）

是一種**模擬演練**，透過討論和假設情境，來驗證組織在面對突發事件時是否有清楚的應變流程與分工。它不需要真的中斷服務或造成損害，而是讓各單位成員在安全的環境下「演練思考」，當遇到資安事件或營運中斷時，大家能否照著計畫行動、找到問題並加以改進。

模擬情境例如：

- 官網、預約系統、捐款平台全面停擺
- 系統與資料庫無法連線
- 門口排滿遊客，要求退票或改期
- 合作的非營利組織研究報告無法即時上傳
- 財務金流暫停，捐款收不到

④ 改善不是一次到位，而是持續循環

資安制度不是寫完就束之高閣的文件，也不是喊了就會實現的口號。透過稽核、和桌上推演，找出現行制度的漏洞並改善，不是為了挑刺，而是為了在每次遇到問題時，我們會主動去想：要怎麼改，怎麼做更好，將「發現」轉化為「行動」，補強制度、避免同樣的錯誤重演。

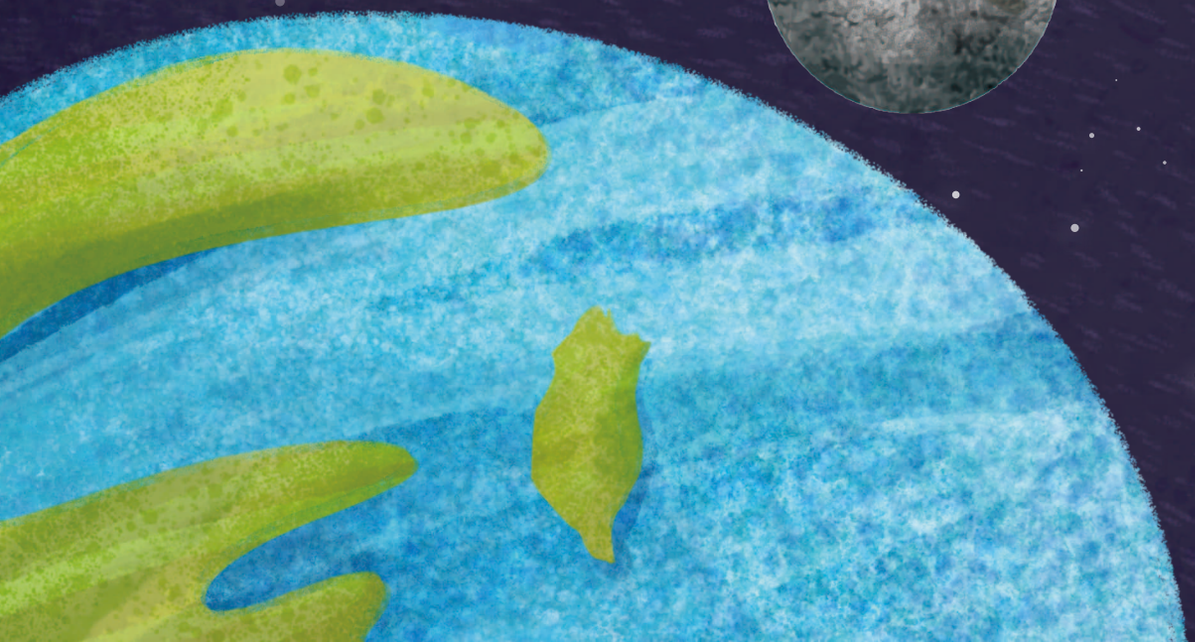
詳細解釋和更多 BCP、桌上推演說明
請見《星際資安指南：資安制度全攻略》

- 結 語 -

每個人都是資安宇宙的守護者

翻開《資安星際指南》，我們不只跟著椒魚探訪各個星球，也在為自己的組織啟動一場旅程；從最基礎的收發信件、到更嚴謹的資產盤點，每天工作的現場都有必須留意的資安防護。資安從來不是「一次完成」，而是隨著環境持續更新與調整的過程。

對多數中小企業與非營利組織而言，資安不用艱深，也不必然昂貴。它並非僅屬於資訊人員的專業，更存在於每個日常操作與工作習慣中。懂技術的人固然重要，但眞正撐起防線的，是願意多想一步、彼此提醒的每一位夥伴。



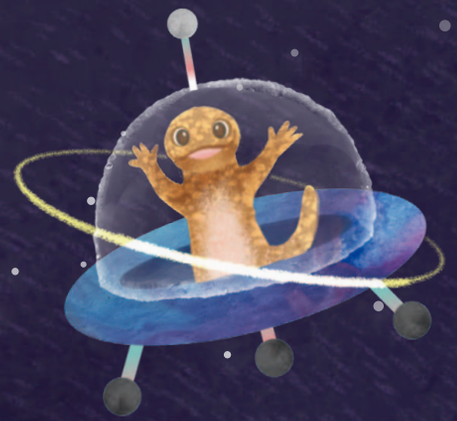
組織文化，是資安能長久運作的基石

再嚴密的制度、再昂貴的系統，若難以遵守或疏於維護，也會逐漸失靈；若沒有「知道為什麼」與「願意去做」的文化，資安也難以維繫。當人人理解自己的角色，主動保護資料、彼此支持提醒，資安就成為組織穩定運轉的推力。

讓我們從今天開始
啟動「資通安全航行」的日常任務

- 寄信前，檢查附件與收件人。
- 安裝新設備時，變更預設密碼。
- 面對語氣急促的可疑郵件，停下手指，多想一秒。
- 定期備份與演練，預想資安事件來襲時如何應變。
- 留下紀錄與改進，讓下一次應對更快更好。

每一個細微的動作，都是一層重要的防護罩。讓我們從日常行動落實資安，成為組織內彼此最堅定、也最可靠的夥伴。



《資安星際指南: 航程導引》

出版單位　國家資通安全研究院

召 集 人　林盈達

主　　編　許建榮

副 主 編　方耀宇

執行編輯　胡馨元

作　　者　邱元貞、張恩鳳、陳思帆、魏鈞培

設　　計　施逸青

出版日期　2025 年 12 月　初版一刷

ISBN　978-986-5436-78-0

本手冊出版來自 NICS 台灣資安計畫，由 Google.org 提供資金挹注。

國家資通安全研究院
National Institute of Cyber Security

with support from Google.org

ISBN: 978-9-86543-678-0