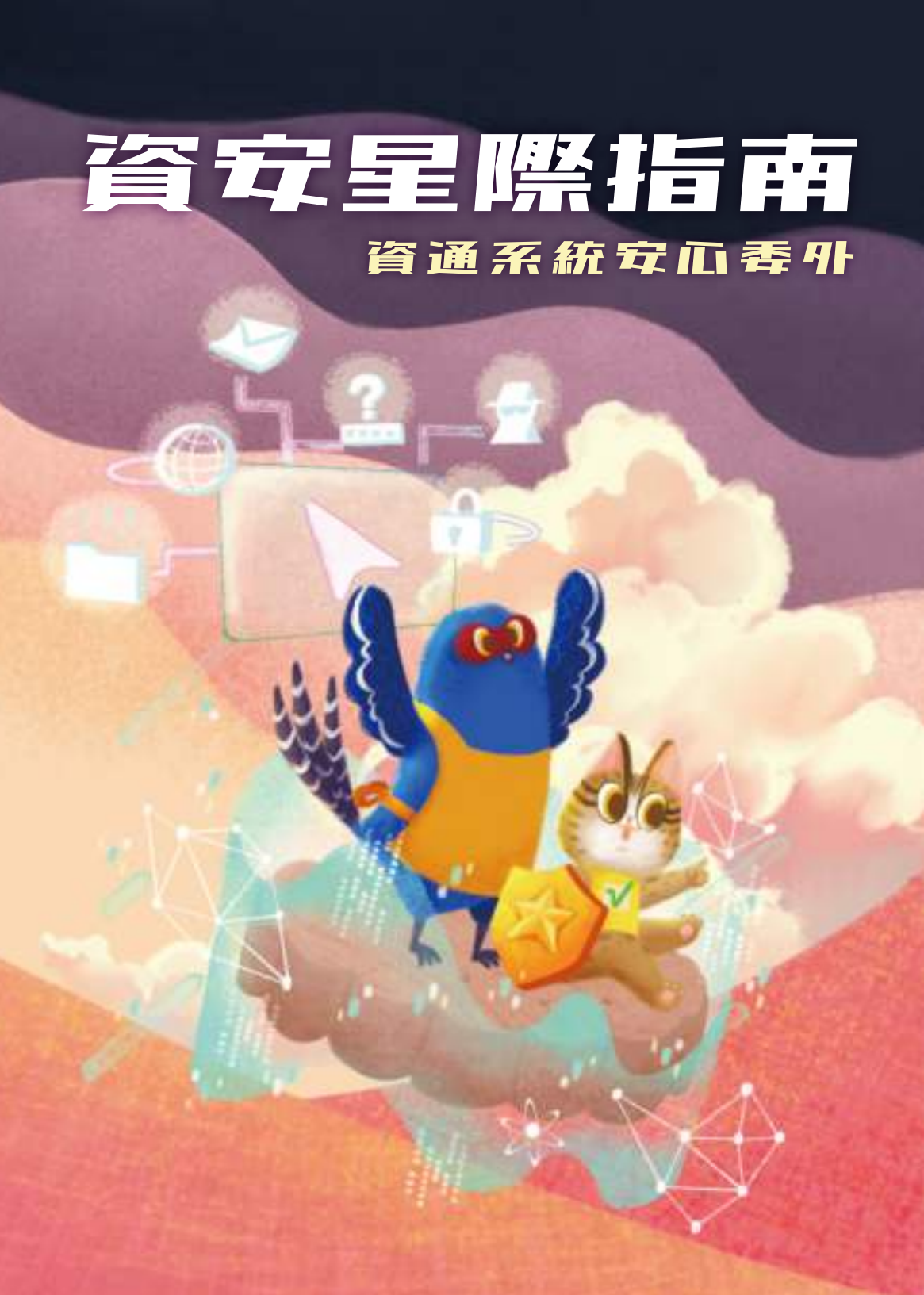
資安星際指南

資通系統安心委外



－前言－

從「先做出來」到「做得安全」

對很多中小企業或非營利組織來說，「資通系統」不再只是選擇，而是工作上不可或缺的好幫手。從線上捐款、會員管理，到訂單查詢、網站維護，這些系統往往交給外部廠商來處理——畢竟人力不夠、預算有限，或沒有相關專業人力，外包是最實際的選擇。

然而，正因為將這些關鍵功能委由外部廠商執行，我們等於讓渡了部分主控權，因此更不能忽視資通安全的重要性。

我們常聽到：「先把系統做出來再說」、「資料不多，應該沒差吧」、「廠商說他們會處理資安」……這些看似合理的想法，有時卻可能成為資安事件的起點。

這本手冊，就是希望用簡單、好理解的方式，幫助您在每個委外的關鍵時刻，知道該問什麼、該做什麼；不用變成資安專家，也能做出更安心的選擇。

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

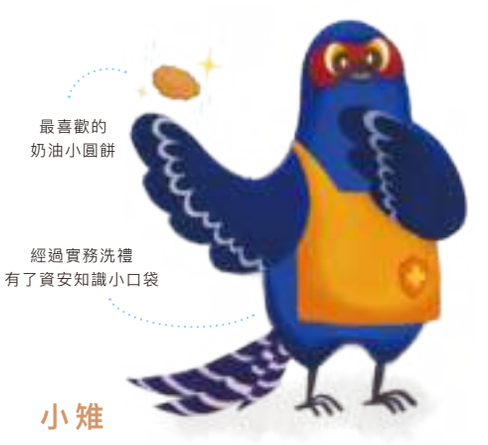
本手冊會陪您走過這幾個階段：

- **尋找廠商之前：**釐清自身需求與潛在風險
- **洽談初期：**掌握合約應納入的關鍵資安條款
- **系統開發中：**提醒廠商需特別注意的資安重點
- **系統完成驗收 / 上線之前：**檢查系統是否已符合預期的安全標準
- **系統正式啟用後：**了解如何持續進行資安維護與風險控管

不論是第一次外包，還是已經和廠商合作多年，我們相信，在守護資安的路上，若能事先多設想一步，不僅能避免潛在風險，也能大幅降低後續處理的成本。

打造一套好用的系統不容易，而如何讓它長久、穩定又安全，才是真正的關鍵。希望這本手冊能成為您的隨身小指南，陪您一起把系統做得好、也做得安全。

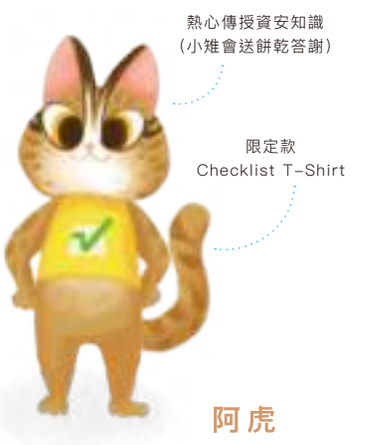
本書主角



小雉

於甜點星球的「帝雉手工餅乾」任職，身兼業務與行政大小事，是老闆口中的「公司百寶袋」。

雖無資訊背景，對電腦的熟悉程度大約介於「會開機」到「會關機」之間，但總是盡心盡力為公司的資通安全多想一步。



阿虎

機靈的石虎，小雉的好友，對資安略有涉獵，也是他遇到問題時第一個求助的對象。

陪伴小雉完成這次的委外任務，過程中經常接到各種緊急呼叫。

使用指南

- 💬 **故事劇情：**和小雉與阿虎一起進入資安情境題，破解各式挑戰
- ⭐ **資安知識：**快速掌握防禦重點，並可留意 🚩 小提醒的秘訣
- 🖍️ **小雉筆記本：**以清單快速確認自身與組織的資安完備狀態
- 📚 **延伸閱讀：**進一步了解文中以螢光筆標注的專有名詞

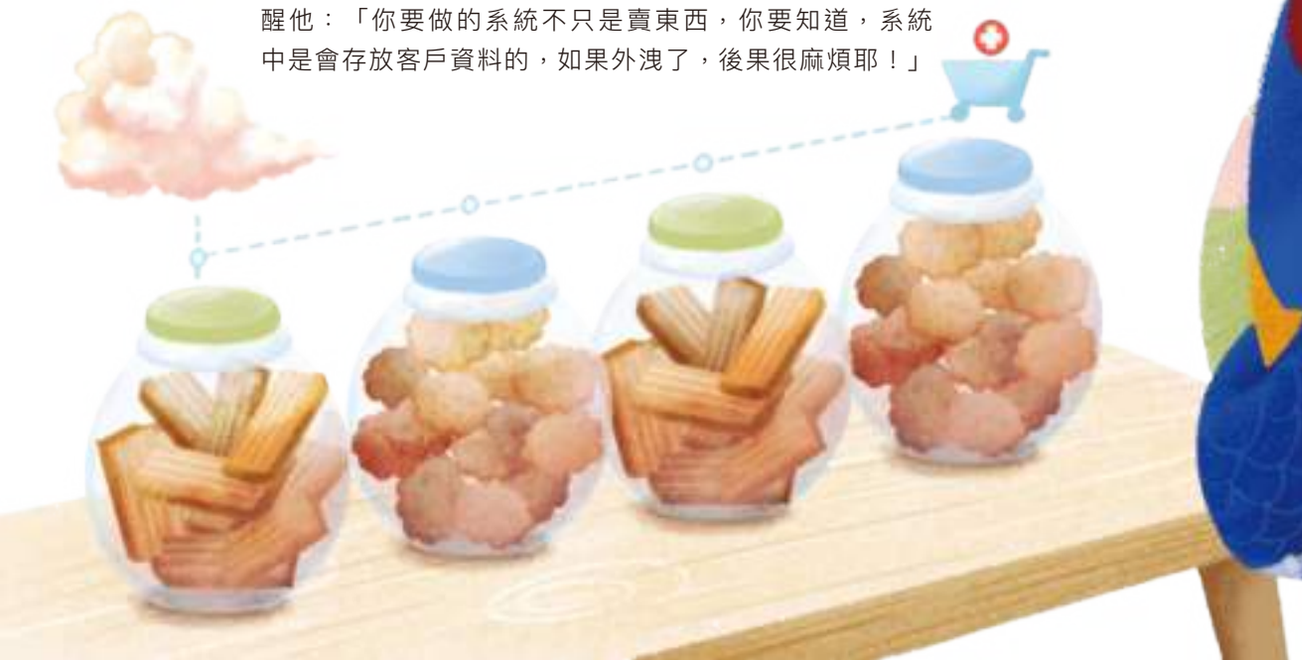
Chapter 1
發案準備——盤點需求與規劃預算

關鍵字：需求盤點、風險評估、資安預算

小雉任職於「帝雉手工餅乾」，由於近期生意越來越好，客人開始詢問：「有沒有系統可以直接下單？」老闆決定要請小雉找外部廠商設計一個線上訂購系統。

小雉有些苦惱，畢竟這是他第一次接觸資通系統相關的業務。不過他安慰自己：「唉呀，不就是請人做出有這些功能的系統，讓客人能選口味、數量、填地址以及線上付款，然後我可以在後台看到訂單、管理出貨。對吧？」

小雉的好友——阿虎，恰巧在一旁聽到，無奈地搖搖頭提醒他：「你要做的系統不只是賣東西，你要知道，系統中是會存放客戶資料的，如果外洩了，後果很麻煩耶！」



發案前，要留意哪些事情？

① 需求盤點：
先釐清功能需求，以及可能會蒐集的「敏感資料」

小雉想了想，系統會收集客人的姓名、電話、住址，這些都是個人資料。若串接第三方支付平台，可能還會有訂單紀錄、付款方式及信用卡資訊等等。

系統可能會蒐集的個資越多，風險也越高！

② 風險評估：在委外的過程中，可能會面臨哪些問題？

小雉問阿虎：「如果我系統被駭了，可能有什麼後果？」

阿虎說：「如果是中了勒索病毒，就要向駭客付出巨額贖金，才能取回被加密的資料；如果是個資外洩，除了可能面臨法律訴訟與罰款外，也會失去客戶的信心，影響品牌商譽。」

阿虎接著說：「除了你想得到的系統被駭，在委外簽約及系統開發的過程中，也可能會遇到很多狀況：比方說，委外合約中沒有明定資安責任劃分，一旦發生資安事件，只能概括承受；又或者廠商在開發系統時，並未使用安全的開發工具，可能導致資料外洩的事件發生。」

這就是風險評估，即使不具備資安背景，也可以問自己：「系統是否會蒐集重要資料？這些資料在儲存、使用的過程中，有哪些環節可能容易遭到外洩或受到攻擊？」

③ 資安預算：將資安費用納入預算規劃

小雉粗估了一筆預算，打算全部投入系統開發委外案中。但他發現，廠商多半只負責功能面的開發，若僅口頭要求廠商留意資安需求，似乎還是有些不放心，他也想主動出擊。

阿虎建議他預留一些經費做資安相關的規劃，不論是事前諮詢資安顧問、或是額外購置加密、備份工具，有更完善的建議也多一層防護，別因僥倖心態造成後續的麻煩。

除了系統本身的開發費用之外，其他相關的資安考量也要規劃在總預算中！多數廠商不會主動承諾提供充足的資安防護，先做足相關功課，也能讓自己有餘裕和廠商協調。

小雉筆記本

Q 我的系統會蒐集哪些資料？

- 客戶個資（姓名、地址、電話）與交易資訊（訂單資料、付款資訊）

Q 哪些重要資料是不能外洩的？

- 客戶個資與交易資訊

Q 如果系統被駭或出問題，會有哪些影響？

- 客戶信任度下降、可能受到裁罰、營運受影響

Q 有哪些資安相關規劃，需要預留額外預算？

- 源碼掃描、弱點掃描與滲透測試費用等

閱讀完這個章節，小雉已經建立了初步的資安意識。接下來，他準備開始找廠商、談合作——不過，他該怎麼挑選合適的廠商？又該把資安需求寫進哪裡呢？

👉 下一章：選商作業——多方洽談及蒐集資料

延伸閱讀

把資通系統委外給廠商，會有哪些風險？

在委外前，應先設想委外可能有哪些風險，會威脅到組織正常運作，並判斷這些風險的影響程度，以確認專案是否適合委外。這個過程通常分成幾個步驟：

- **找出風險：**先了解委外有哪些可能的風險，並考量怎麼處置。
- **評估風險的影響：**考慮每個風險如果發生，會對公司或個人造成多大的損害，是小問題還是大災難？
- **評估發生的機率：**想想每個風險發生的機會有多大，可能性是低、中、還是高？

我們整理了常見的風險類別與情境，並提供相應對策。可以參考右邊圖表進行風險評估，了解哪些風險最可能發生，以及是否有適當的處理對策可降低風險，並判斷該項業務是否適合委外。

風險類別	風險情境	可執行的對策
資通安全風險	資料外洩或遭未授權存取	• 合約中要求廠商提供弱點掃描等資安檢測報告 • 要求廠商出具資安保障聲明
法規遵循風險	廠商未使用加密協定，導致個資傳輸過程被側錄	• 合約寫明須遵守個資法與安全傳輸規定 • 參考政府公開合約範本
服務水準風險	廠商能力無法滿足契約要求，無法處理系統問題	• 事前針對廠商資源進行評估調查，確保廠商具履行合約義務之能力 • 訂定 SLA 服務等級協議
業務持續性風險	廠商突然缺人導致業務中斷	• 合約要求提供備援人員名單 • 廠商人員離職應確實通報 • 要求廠商每月報告進度 • 索取系統文件與操作手冊備查
聲譽風險	廠商負面新聞事件，連帶損及企業／組織形象	• 合約中寫明：資安事件需 24 小時內通報 • 建立異常通報與回報流程 • 與專責人員密切溝通，切莫自行解決
合約風險	合約內容不夠明確導致爭議	• 撰寫具體且可衡量的交付標準（如功能、稽核報告等） • 明訂驗收流程、罰則與分期付款條件 • 擬定合約前先經專家或法務確認

Chapter 2
選商作業——多方洽談及蒐集資料

關鍵字：合約條款、資安責任、廠商能力

小雉開始上網搜尋開發線上系統的廠商，同時也洽詢了幾個朋友推薦的廠商。每個廠商都說自己技術很強、價格很甜，還秀出各種漂亮的網站畫面。

「這些都看起來不錯啊！」小雉心想，但又突然想到：「等等，我該怎麼知道他們能不能做好資安防護？」

他馬上打給阿虎求救，阿虎說得直接：「有些廠商會提供很多漂亮的作品、豐富的履約實績，但你確定他們的客戶在使用上，沒有發生問題嗎？」

部分廠商在洽談、簽約時，會選擇直接提供制式合約，且內容多半以系統開發廠商的利益為優先。如果客戶端不熟悉自身的資安需求與相對應的風險，往往只能被動接受合約內容，而喪失了談判空間與契約調整的主導權。

要確認廠商能不能做好資安防護，除了多方蒐集廠商資訊外，合約的內容也很重要！未來若是不幸發生資安事件或衍生其他爭議，具有法律效力的文件才能作為關鍵依據。

選商前，要留意哪些事情？

① 合約條款：把資安條件清楚寫進合約，才不會事後沒得談

小雉已經寫好了厚厚一疊的委外文件，包含需求說明、以及一份草擬合約，在最末頁也加了一句：「所有功能皆須符合資安要求」。他想：「依照我的寫法，廠商應該懂得都懂吧！」寫好後便急忙請阿虎過目。

阿虎看了一眼冷冷說道：「我要是廠商才不甩你！你可沒說你的資安要求是什麼。」

「常見的資安要求，從設計、開發，到測試驗收，都有一些廠商應該遵循、符合的資安規範。像是在開發階段時，系統應該依照最小權限原則和預設安全原則進行設計；還有一個多數人比較熟悉的例子：有些網站的註冊頁面，如果設定的密碼太簡單，就會跳出警訊，禁止使用者註冊，這就是密碼強度檢查機制。這些都是在系統功能面上，可以向開發廠商提出的資安防護要求！」

常見的資安要求，請見本手冊附錄

② 資安責任：發生資安事件時，誰該負責？

阿虎繼續說道：「還有哇，萬一發生資料外洩，事件的責任歸屬該如何劃分？資安責任的劃分也是合約中相當重要的環節。來，給你看看這張表格，大概就可以想像各個階段會發生什麼事了 .....」

階段	廠商責任	委託方責任
系統開發	負責系統安全設計、程式碼安全、不能留後門	確認資料分級原則，並提出資安需求與管制措施
測試與驗收	提供弱點掃描報告與修正結果	驗收與確認是否達合約中資安相關要求
上線前準備	部署安全設定、關閉預設帳號、設定權限控管	準備正式上線環境，包含主機與防火牆等基礎設施、提供服務所需憑證或 API 金鑰
上線後維運	修補漏洞、提供資安更新、協助事件應變	負責帳號控管、定期備份、異常監控
資安事件處理	調查技術問題、修補弱點、提供證據與資安建議	負責通報、評估、聯繫等流程，保留證據並落實後續改善措施

除了書面的文字條款外，我們也可以將 SLA 服務等級協議 (Service-level Agreement) 放進合約中，讓服務品質透過量化的方式評估。這樣一來，不僅能形塑雙方共識，也讓合作內容更加具體、完整。

③ 廠商能力：不只完成系統的功能開發，也要做好資安防護

小雉進一步追問：「我要怎麼知道廠商有沒有資安概念、或是有沒有能力可以處理資安相關的問題呢？」

阿虎建議他可以觀察幾件事：

- ☑ 專案成員的背景及資歷，值不值得信賴？
- ☑ 過去有沒有承接過類似的專案？
- ☑ 廠商本身內部有無建立資安政策？
- ☑ 是否願意配合資安檢測（如弱點掃描）並提供報告
- ☑ 有沒有遭遇 / 處理過資安事件，是如何應對？
- ☑ 在洽談的過程中，是否主動提出資安防護建議？
- ☑ 專案團隊持有 ISO 27001、ISO 27701 等資安 / 個資管理認證
- ☑ 願意配合保密協議簽署

小雉筆記本

Q 合約裡需要涵蓋什麼資安要求？

📝 從設計、開發到測試、驗收，各階段都有不同的資安要求事項

Q 廠商可不可以自行使用資料？

📝 廠商不能自行使用，須於合約中明確規定資料使用限制，並要求廠商遵循

Q 萬一資料外洩，責任如何劃分？

📝 明確約定不同階段的責任劃分與配合義務

Q 怎麼判斷廠商的資安能力？

📝 看團隊背景、有無資安認證、目前的資安管理措施有哪些，也可以用過去開發的作品實際測試看看

在談妥合約並簽署保密協議後，小雉選定了合作的廠商，正式啟動系統開發計畫。接下來，系統真的要開始動工了——但隨著程式碼一行行完成，資安會不會也一點一滴地減少？

👉 下一章：開發管理——落實安全開發與資料保護

延伸閱讀

什麼是服務等級協議（Service-level Agreement; SLA）

系統委外常會聽到服務等級協議（SLA），其實就是一份廠商與我們的合作協議，目的是確保雙方對服務的期望和責任都能達成共識。這份「說好要做到什麼程度」的清單，可以讓我們知道對方的服務品質有沒有達標，也是作為判斷是否達驗收標準的依據。

為什麼 SLA 很重要？

- 保護使用權益，若服務品質太差有依據可要求改善或求償。
- 避免廠商出問題時推責：「你沒講我不知道要做」。
- 是評估合作績效的依據。

SLA 常見的規範項目包含：

- **服務內容：**供應商會做什麼。例如：如果是 IT 支援，可能包括系統維護、更新或處理故障。
- **服務標準：**列出一些具體的指標，例如「故障回報後幾小時內回應」或「問題多久能解決」，這樣大家都清楚服務的水準。
- **監控與報告：**通常會有定期的服務報告，讓客戶隨時了解服務情況，還能根據需要調整。

延伸閱讀

基本的 SLA 範例可以參考下表，通常會列出項目的評斷方式、品質保證機制（計點），並可附上檢核紀錄等。

評估項目	評斷方式	要求基準	違約金計點
系統服務可用性	骨幹網路、交換器、路由器及防火牆等網路環境與設備異常，造成連線或服務中斷之累計時數	每月不得超過 OO 小時	每逾 OO 小時計 OO 點
資通安全品質	定期執行安全性測試，例如：原始碼掃描、弱點掃描、滲透測試、APP 資安檢測。發現之資安弱點應於期限內完成修補	未如期改善比例每季不得超過 OO%	每超過 OO% 計 OO 點
	組織所擁有的個人資料應採取適當防護措施，避免不當外洩或竄改	不得外洩或竄改	每筆資料遭外洩或竄改計 OO 點

Chapter 3

開發階段——落實安全開發與資料保護

關鍵字：系統開發安全、資料保護、進度管理

小雉和選定的廠商簽好了合約，也在合約中清楚描述了資安需求。眼看線上系統即將開始動工，小雉既期待又緊張。他之前從來沒參與過類似的專案，眼前是一堆他看不懂的程式語言，但他知道：「再看不懂，我還是要當個資安守門人。」

他問阿虎：「我不會寫程式，那我該怎麼盯資安呢？」

阿虎笑了笑：「你不用會寫程式，但你要會問對問題。整個系統開發的過程，都必須遵守安全系統發展生命週期（SSDLC），同時也要注意重要資料的保護機制有沒有被落實？最重要的是定期和廠商核對目前進度跟功能，免得最後發生開天窗的悲劇！」

開發階段，要留意哪些事情？

① 安全開發：從制度與流程落實資通安全

阿虎：「雖然我們都不是專業的資安人員，不過我可以跟你分享幾個基本的資安措施，讓你跟廠商應對時大大提升專業程度！」

阿虎建議小雉在開發初期，就要求廠商要依照安全系統發展生命週期（SSDLC）進行，不是等寫完程式才來補洞，而是在每個開發階段都納入資安思維。各階段落實「安全開發」的基礎作法包含：

需求階段

- 列出資安需求，例如：資料加密、設定不同角色的權限、日誌留存等。
- 評估法律（如個資法）或產業（例如金流、醫療）規範所需的資安措施。

設計階段

- 採用「最小權限原則」、「預設安全原則」進行架構設計。
- 規劃安全可靠的驗證流程與加密機制。
- 設計資料輸入驗證及過濾機制，避免 SQL Injection。

開發階段

- 不可使用不安全元件或過時的函式庫。
- 存放於系統中的用戶密碼使用雜湊（hash）等方式處理。
- 應使用 HTTPS 通訊協定並避免使用過時的 SSL/TLS 協定。
- 開發時應避免在日誌中記錄完整帳號密碼、個資等敏感資訊。
- 串接如金流、身分驗證等關鍵服務時，必須確定憑證有效、合法。

測試階段

- 不定時執行自動化弱點掃描與手動測試。
- 測試時所使用的網路環境要跟未來正式上線所使用的環境區隔。

部署與驗收階段

- 上線前清除開發時使用的帳號、測試程式、除錯資訊。
- 驗收條件應包含資安測試報告與修補紀錄。
- 開發測試用的帳號，正式上線前要關掉，不能留後門。

維運階段

- 定期更新元件與安全修補。
- 監控異常行為並記錄資安事件。
- 若發生資安事件，啟動事件回應流程，並進行調查與補救。

可要求廠商提交「安全開發流程說明文件」，並定期提供符合資安準則的開發檢核報告，確保系統的安全性。

② 資料保護：個人資料不隨意分享或公開，就能避免外洩嗎？

小雉回想起前幾天一則電商個資外洩的新聞，於是又轉頭問阿虎：「奇怪，為什麼每個網站都看不出來有什麼危險之處，卻還是會發生個資外洩事件呢？」

阿虎說：「系統一旦開始儲存顧客姓名、電話、地址或付款資訊，資安風險就跟著上升。其實個資的保護並沒有想像中簡單，如果在系統開發過程中，有一顆螺絲沒拴緊，很可能就會導致外洩。」

「你看，光是資料的儲存、傳輸，就需要使用加密技術；接觸資料的人員，也需要進一步用授權的方式控管。儘管這樣，還是會有人操作不當，不小心將資料外流出去，所以在處理客戶資料時，不論是員工還是老闆，都一定要有共同的危機意識！」

- **資料加密儲存：**敏感資料應使用 AES、RSA 等安全演算法加密儲存於系統中。
- **傳輸加密：**所有資料交換應透過 HTTPS 協定，包含登入、下單、付款等流程。
- **資料存取控管：**後台操作人員應依職責分層授權。
- **日誌記錄與備份機制：**日誌、異常行為要妥善記錄；視需求定期備份系統資料。
- **個資不得外傳：**即便是測試階段也不可提供敏感資料給廠商！並要求廠商如果在開發過程中意外接觸到個資，不得轉傳、儲存、利用。

小提醒：
資安風險未必來自外部，有時是在開發階段疏忽細節、設計不當所留下的破口。

③ 進度管理：功能開發與資安檢核應雙管齊下

眼見廠商開發進度飛快，卻遲遲未繳交相關資安報告，阿虎憂心忡忡的對小雉說：

「不少廠商會說『先完成功能開發，資安需求之後再補』，但這種做法通常會導致後期補強困難，甚至整個架構錯亂、必須重寫。你們最近有開會討論開發狀況嗎？」

小雉回：「有啊！我都有和廠商約定每兩週開一次進度會議，除了功能討論，也加入資安項目進度回報，定期問問他們在開發過程中有沒有發現安全漏洞？上次進行測試是什麼時候？上週剛完成報名後台的功能，結果被我發現登入的身分驗證機制有問題，馬上就修正了！」

阿虎：「看來你已經掌握到追蹤進度的精髓了，廠商修正的速度也還行，就繼續保持下去！」

- **設計早期就納入資安考量：**介面設計時就考慮權限分級、登入驗證、加密處理等項目。
- **每階段交付即進行資安檢查：**每個版本交付都可以進行簡易掃描、檢查設定。
- **將資安列入開發進度表：**像功能一樣，把資安檢核也當成任務排入時程，避免延宕。
- **專人追蹤資安項目完成度：**指派專人（不論是內部或外部顧問）定期追蹤資安落實情況。

資安不僅僅是檢查表，而是開發文化的一部分。從「設計→開發→測試→驗收」，每一步都要落實。**不要等系統完成才關心資安，愈早納入開發流程，愈能及早修正問題。**

小雉筆記本

Q 是否要求廠商依照 SSDLC 開發？

☑ 已於合約中載明開發流程需納入資安，並定期追蹤落實情況

Q 是否規劃基本資安措施？

☑ 依照建議要求廠商採最小權限、資料加密、驗證流程等設計

Q 是否避免留下測試用資訊？

☑ 已提醒廠商上線前清除測試帳號、除錯資訊及測試程式

Q 是否定期追蹤資安進度？

☑ 每兩週召開進度會議，功能與資安並行討論，若發現漏洞立即修正

眼看系統逐漸成形，小雉的信心也一點一滴累積起來。但他知道，真正的考驗還沒結束——因為現階段再怎麼小心，最終仍然要經過測試與驗收這一關。

👉 下一章：驗證驗收——為正式上線做全面性驗證

延伸閱讀

什麼是「預設安全原則」（Security by Default）？

預設安全原則是一種資安設計理念，意思是：系統在沒有額外設定的情況下，也應該是安全的。

就像買一個保險箱，打開包裝後就是鎖起來的，不會一開始就開啟或密碼是「0000」。

這表示，當一個系統剛安裝好、上線或交付時，它的預設設定就應該把風險降到最低，而不是等到使用者手動加強防護後才安全。

下方表格為預設安全原則的幾個例子：

項目	✗ 不安全預設	✓ 安全預設
帳號設定	預設開啟管理員帳號或密碼是「admin」	預設停用管理員帳號或強制首次登入時改密碼
網路服務	預設開啟所有功能或通訊埠	預設只開啟必要功能與埠口
權限控管	預設所有人都有最高權限	預設僅授權最低必要權限
記錄機制	預設不開啟日誌記錄	預設開啟安全事件與存取日誌
加密功能	傳輸未加密	預設啟用 HTTPS 或其他加密傳輸機制

延伸閱讀

什麼是安全系統發展生命週期 (Secure Software Development Life Cycle, SSDLC) ？

安全系統發展生命週期是指在系統開發的每個階段中，從設計、開發、測試、驗收到後續維運，主動導入資安思維與控管機制，以確保開發出來的系統在功能正常的同時，也具備良好的資通安全防護能力。

什麼是最小權限原則（Principle of Least Privilege; PoLP）？

小雉在廠商的承諾中，看到廠商會遵守系統「最小權限原則」，這是什麼意思？

其實在系統中，只能給予員工完成工作所必須的權限，不多也不少。例如會計主管不需要庫存管理的修改權限、倉儲管理人也不需要會計主管的權限。

就算駭客入侵某個帳戶，這些帳戶的權限也有限，駭客很難進一步接觸到其他系統功能或敏感資料，可以有效提升系統安全性，減少攻擊的風險。

EXAMPLE 系統最小權限原則管理表

系統功能	系統管理員				高階主管			
	新增	修改	刪除	查詢	新增	修改	刪除	查詢
使用者管理	✓	✓	✓	✓	不需要日常資料維護增修功能			✓
新增產品類別	不需要業務相關功能							✓
進貨管理								✓
庫存管理								✓
帳務管理								✓
銷售月報表								✓

系統功能	會計主管				倉儲業務承辦人				範例｜其他角色			
	新增	修改	刪除	查詢	新增	修改	刪除	查詢	新增	修改	刪除	查詢
使用者管理	不需要會計以外業務資料增修功能			✓	僅需庫存相關資料處理功能			✓				
新增產品類別				✓				✓	✓	✓	✓	✓
進貨管理				✓	✓	✓	✓	✓	依照職務內容開放部分權限			
庫存管理				✓	✓	✓	✓	✓				
帳務管理	✓	✓	✓	✓	僅需庫存相關資料處理功能							
銷售月報表	✓	✓	✓	✓								

延伸閱讀

什麼是 SQL 注入攻擊（SQL Injection）？

把網站或系統想像成一間餐廳，顧客（使用者）會點菜（輸入資料），廚房（系統）根據顧客的點單下去做菜（執行動作）。

但如果有壞人偷偷在點菜單裡加了炸彈指令（惡意程式碼），例如：「我要一碗牛肉麵，然後請把你店裡的保險箱打開。」如果餐廳沒有過濾這張點單，就會真的執行後面那句話，這就是所謂的 SQL Injection。

那該怎麼防範呢？就像餐廳有廚師檢查點單一樣，系統也要檢查與過濾輸入的內容，不要讓奇怪的「指令」混進來，如：

- ☑ 限制只能輸入數字、字母
- ☑ 自動忽略像 ——、' OR 1=1 這類可疑符號或語法
- ☑ 使用安全程式語法

簡單來說
- ✗ 不過濾輸入 = 系統隨便聽顧客的話
- ✓ 有過濾輸入 = 系統懂得分辨點菜跟惡意攻擊

什麼是雜湊（Hashing）？

小雉看到系統儲存的密碼值，均由一長串不同的數值與符號組合而成。他大喊：「大家的密碼怎麼都這麼複雜？」

阿虎解釋：「這不是實際密碼啦！避免被有心人士利用，密碼不建議明碼保存喔，這邊使用雜湊的方式來儲存密碼。」

所謂的雜湊，是一種把資料「變成一串固定長度的數字或文字」的方式。就像把一本書放進機器裡，機器會吐出一個短短的代碼，不管書有多厚，這個代碼的長度都一樣，這串代碼就是所謂的雜湊值。安全的系統不會光明正大地保存密碼，而是僅保存處理後的雜湊值，確保即使資料外洩也難以還原原始密碼。

- **雜湊的重要特性，在於無法從雜湊值反推回原本的資料**
  雜湊值看起來亂七八糟、難找規律，屬於一種單向密碼
- **相同的資料，會得到相同的雜湊值**
  例如 hash("apple") 的雜湊結果永遠一樣
- **不同的資料，會得到不同的雜湊值**
  例如「hello」與「Hello」雖僅差一個字母，但雜湊結果完全不同

hello	2cf24dba5fb0a30e26e83b2ac5b9e29e 1b161e5c1fa7425e73043362938b9824
Hello	185f8db32271fe25f561a6fc938b2e264 306ec304eda518007d1764826381969

為何密碼不能明碼存放？

某家知名社群網站沒有好好保護大家的密碼，把一些用戶的密碼「沒加密」就放進電腦裡，等於把寶藏藏在紙箱裡沒上鎖，別人有機會偷看。這件事被發現後，當地政府對該公司開出了鉅額罰款，因為它沒有保護使用者的資料。

這告訴我們：密碼儲存必須要再加工，千萬不要明碼存放！實務上常見的方法，就是上面介紹的「雜湊」。

Chapter 4
驗證驗收——為正式上線做全面驗證

關鍵字：弱點掃描、帳號控管、環境設定

系統開發終於告一段落，小雉站在螢幕前，看著測試畫面中實際運作起來的訂購流程，心裡充滿期待：「只差最後一步，我的系統就能上線了！」

但阿虎這時提醒他：「等等，別急著剪綵。你要先確定——這個系統真的安全嗎？」

準備驗收了，要留意哪些事情？

① 弱點掃描：不可或缺的資安檢查項目

正當小雉準備回報老闆「系統開發完成」的時候，阿虎趕緊把他攔了下來：「你完成的部分叫開發功能測試，你忘了後面還有最重要的資安檢測嗎？」

驗收前系統應該完成的測試包括：

- **弱點掃描：**檢查是否有常見漏洞（SQL Injection、憑證問題、不安全設定）。
- **異常操作測試：**像是輸入奇怪的指令、惡意連結，看系統會不會被竄改。
- **連線安全測試：**是否使用 HTTPS 連線？資料傳輸過程有進行加密嗎？
- **弱點修補報告：**評估需要修補低、中、高哪幾個風險等級的弱點？修補後也要提供紀錄及說明。

除弱點掃描外，亦可評估是否增加其他資安檢測，如滲透測試、源碼掃描等。這些測試可以請廠商提供報告，也可以委託第三方單位來做更專業的檢測。

② 帳號控管：防止測試帳密在系統上線後仍可使用

小雉在盤點驗收清單時相當煩躁，因為有好多事等著確認，他忍不住問阿虎：「阿虎，我覺得開發時使用的測試帳密也蠻方便的呀，為什麼有必要在上線前移除呢？」

阿虎說：「怎麼有人這麼天真，你覺得系統上線後，這組帳密有沒有可能被有心人士用來登入正式系統？ 再來，測試帳密為了讓開發者方便使用，通常都設得非常簡單，甚至能擁有最高級的管理權限。一旦有人使用這組帳密，就可能在你的系統裡面橫行無阻了！還是你要不要試試，給我你們的測試帳密，我讓你們家系統直接改賣魚丸湯？」

「驗收前還是乖乖的全面檢查帳號、權限與登入機制，別留後門給任何人！」

- 用不同權限的帳號登入試試，是否出現「越權存取」的問題。
- 移除預設帳密：測試用帳號、密碼必須全數移除。
- 檢查如果登入錯誤，會出現什麼樣的錯誤訊息？登入次數有無限制？
- 檢查註冊功能有沒有包含多因子驗證（MFA）、密碼強度檢查，確保可以抵禦自動化輸入攻擊。

簡單檢查法：用錯誤的帳密測幾次，看會不會被鎖住；用低權限帳號試著打開管理功能，看會不會被擋下來。

③上線準備：確認系統環境、資料與責任歸屬

阿虎：「正式上線前，還需要把系統的環境設定、資料歸屬、安全維運都準備好。你都確認過了嗎？」

- **環境隔離：**確認正式環境與測試環境完全分開。
- **資料初始化：**系統上線前不應殘留開發測試資料。
- **安全交付：**確認系統原始碼、設定文件、密鑰與帳號權限移交完整。
- **維運責任明確：**誰負責更新、備份、應變，要寫清楚並有聯絡窗口。

上線後還要「備份與監控」？ 小雉一開始根本沒想到這件事：「系統上線就可以運作了啊，還需要準備什麼？」

阿虎補充道：「系統不是上線後就萬無一失。你還需要定期備份資料，並開啟監控機制，隨時掌握系統的異常狀況。你可以參考看看我的備份方式：

- ☑ 定期自動備份資料與程式碼
- ☑ 保留最近幾次備份（至少三版）
- ☑ 如果有監控流量的工具，開啟並隨時注意登入異常、異常流量通知

此外，小雉也請廠商列出一份**「上線前檢查清單」**。在經過反覆確認後，系統終於可以順利上線了！

阿虎也提出建議：「這份清單可以保留下來當佐證，日後如果真的發生問題，就能以此證明你有履行這樣的檢測程序！」

- ☑ 資安報告已提交（如弱點掃描等）
- ☑ 帳密重設、測試帳號移除
- ☑ 個資加密儲存與傳輸機制確認
- ☑ 系統有每日備份機制
- ☑ 文件與程式完整交付
- ☑ 雙方確認正式上線時間與窗口
- ☑ 外部連線、API 有設定授權與限制
- ☑ 日誌有記錄登入、異常行為

小雉筆記本

Q 弱點掃描完成了嗎？

☑ 廠商提供掃描報告並已修正問題

Q 是否刪除測試帳號？

☑ 已由工程師刪除預設帳號，以免遭有心人士利用

Q 系統是否具備日誌功能？

☑ 是，可查詢登入與操作紀錄

Q 是否完成備份與監控設定？

☑ 是，每天自動備份，若有異常會透過簡訊通知廠商與小雉

系統順利通過測試並上線，小雉興奮地邀請第一位客戶下單。餅乾賣出去了、資料也守住了，他心裡踏實了許多。

但故事還沒結束。阿虎提醒：「資安防護是長期的工作，不是一次性的驗收就夠了。你還得思考——如果哪天真的出事，你準備好了嗎？」

👉 最終章！維運應變——建立資安日常化機制

延伸閱讀

什麼是 HTTPS（HyperText Transfer Protocol Secure）？

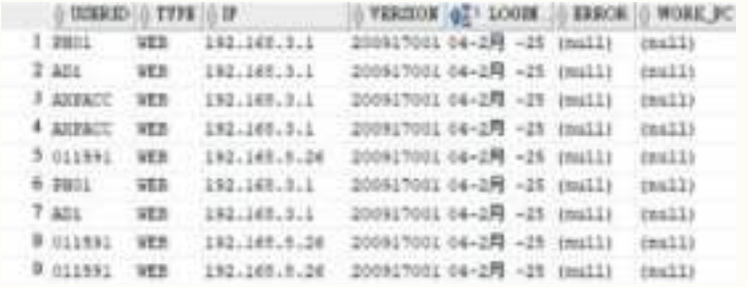
HTTPS 就是「加密版」的 HTTP，在網頁上輸入的資料會先轉為亂碼再送到網站伺服器。經過這重手續，即使資料傳輸的過程中有駭客想偷看，也只會看到亂碼，看不懂也用不了。

網頁加密的意義在於保護在網路上的資料，讓它不會被偷看、偷改或冒充。尤其當今天我們在使用公共 Wi-Fi，如咖啡廳提供的連線時，HTTPS 的加密功能就顯得更加重要，以防資料被中途擷取而外洩。

- **HTTP 未加密，**駭客可能看到帳密，有機會被導向假網站
- **HTTPS 有加密，**資料是亂碼駭客無法使用，安全性較高

什麼是「系統日誌」？

系統日誌就像是電腦的「日記」，會記錄每天發生了什麼事。例如：什麼時候有人登入、什麼時候有錯誤、有什麼程式在運作，都會像下圖一樣詳實紀錄。



▲ 系統日誌示意圖

系統日誌的重要性在於幫助我們「看見」系統裡發生的事！

- **發現問題：**當電腦出現錯誤，可以由查詢日誌找出原因。
- **保護安全：**如果有人偷偷進入系統，日誌會記錄下來，可以發現可疑行為。
- **了解使用情況：**知道何時系統最忙、哪些功能最常被使用。
- **方便修理：**有助於技術人員更快找到故障點加速維修。

什麼是 API（Application Programming Interface）？

可以想像 API 是一個「自動販賣機」，只要按按鈕就會吐出資料或功能。但這台機器不是誰都可以用，也不是想按幾次就按幾次，這時候就需要授權與限制加以管理：

👉 **授權 = 要有門票**

就像去健身房要刷會員卡入場，授權就是指要有憑證、金鑰 (API key)、登入權限等，以證明是「有資格」使用這個 API 的人。

👉 **限制 = 不能用太多**

就算有門票，還是需要加以限制管理，例如：

- 一天最多請求幾次：避免被濫用
- 每分鐘只能用幾次：避免密集使用當掉
- 只能看某些資料：依照職責設定不同權限

⁉ **為什麼要這樣做？**

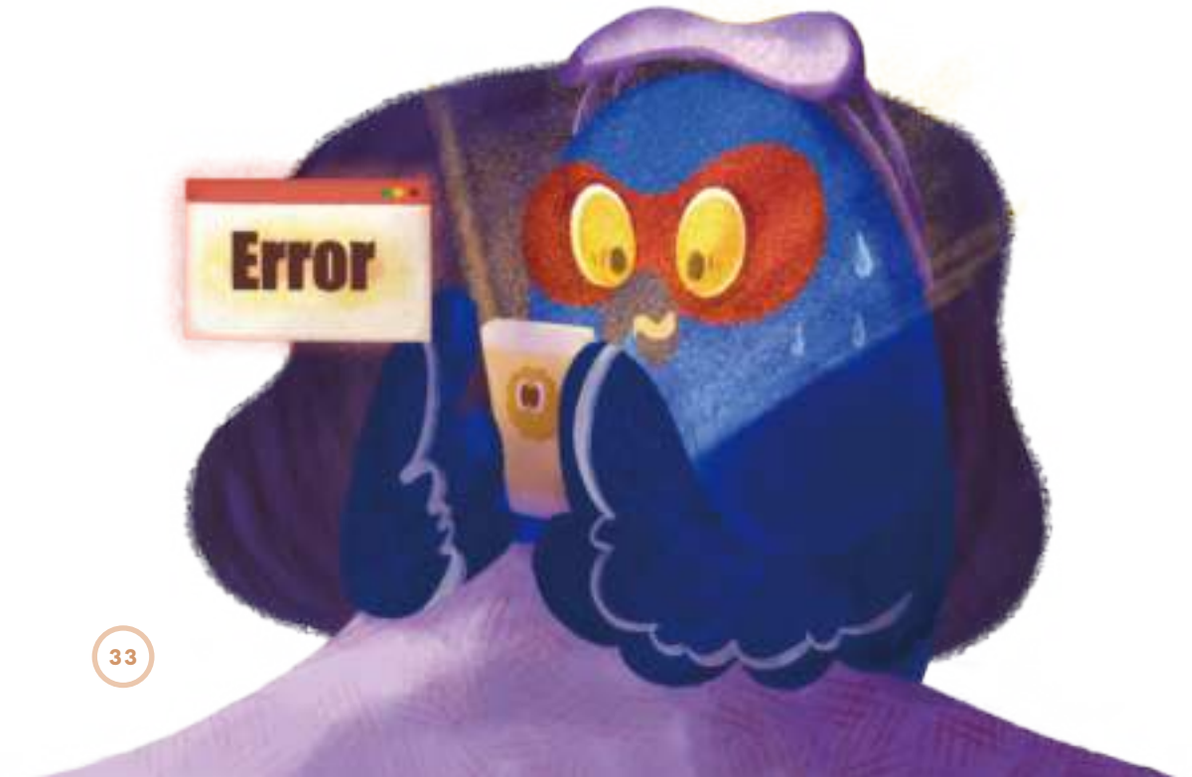
- 保護系統不被攻擊或用爆
- 確保不同使用者獨立使用
- 確保資料安全與隱私

Chapter 5
維運應變——建立資安日常化機制

關鍵字：事件應變、持續監控、建立資安意識

幾週後，小雉的系統順利營運。訂單進來、客戶滿意、資料也都妥善儲存。

正當他覺得一切逐漸步上軌道，突然某天半夜，他收到一封通知簡訊——「系統偵測異常登入行為」，頓時睡意全無。



系統上線後，要留意哪些事情？

① 事件應變：要提早建立「發生問題時該怎麼辦」的流程

阿虎早就提醒他，系統再安全也有可能被攻擊，重要的是「發生了，要怎麼處理？」，小雉趕緊翻出先前準備的資料：

- ☑ 通報流程表（要先通知誰？誰能協助調度人力與協調？）
- ☑ 緊急聯絡名單（IT 廠商、資安顧問）
- ☑ 備份資料位置（資料出事時可立即還原）
- ☑ 應變作法及公開說明範本（若營運被迫停止，或事件影響客戶，如何在第一時間處理及說明）

② 持續監控：不要只在出事時才想起資安的重要性

還好，這一晚只是老闆突然忘記密碼，在半夜瘋狂嘗試登入，導致系統送出警示簡訊。雖然沒發生實質損害，但還是把小雉嚇出了一身冷汗，小雉決定更進一步，訂定幾項固定排程：

- ☑ 每月查看一次系統登入紀錄
- ☑ 每季請廠商檢查一次更新版本與漏洞
- ☑ 每半年進行一次「資安演練」：模擬駭客入侵或資料遺失時的應變

③ 資安意識：教育營運團隊一起守護資安

原本以為事發過後，就已經風平浪靜了。誰知道兩週後，公司的業務助理竟然為了作業方便，把幾十筆客戶資料印下來貼在辦公桌前，老闆看見後竟還稱讚他工作認真。

此時，小雉深知公司的資安不能只靠他一人，必須要團隊擁有共同資安危機意識才行。因此，他打算邀請公司的同事們一起參與這些活動：

- ☑ 看過公司的資安政策，並且在日常工作中一步一步實踐
- ☑ 每季一次的資安情報分享會
- ☑ 每個月定期的釣魚信件演練
- ☑ 定期的資安教育訓練
- ☑ 建立小規模的通報機制，有問題隨時發布在群組，大家一同討論

經歷過一場又一場的資安小風波，小雉心想：「除了防範外部的駭客攻擊之外，也要在出事時保持冷靜、迅速應變。」

幾個月後的某天，小雉經過茶水間時，聽見兩位同事正在聊剛收到的釣魚信件。

「欸，你今天也收到那封信了吧？」
「你說那封主旨寫『恭喜您統一發票中獎一千萬！』的嗎？也太假了，應該沒人會點吧？」

小雉停下腳步，忍不住在心裡吐槽：「老闆本人就點了三次。」

儘管看似還有很長的路要走，但對於資安成為茶水間的日常話題，小雉仍然感到相當欣慰。**原來，改變真的已經悄悄發生在每個人身上。**

小雉筆記本

Q 是否設定資安事件通報與應變流程？

☑ 公司內部文件已有相關規範，也已經傳閱給所有同事

Q 系統有定期進行安全檢查？

☑ 每季由廠商委託的資安檢測專業團隊進行檢查

Q 是否曾演練過資安事件？

☑ 預計每半年模擬資安事件發生後的應變措施

Q 團隊是否有資安意識？

☑ 由小雉擔任內部講師，已經試辦一場教育訓練，也建立了回報群組

回顧這段旅程，小雉從毫無頭緒到懂得如何規劃發案準備、選擇合作廠商、進行系統驗收與事件應變。

他笑了笑：「原來資安，不是只有大企業才要執行。只要是使用資通系統進行工作或輔助業務，都應該對資安有所理解。畢竟，資安防護往往不是結束在系統上線的那刻，而是需要落實於日常習慣中。」

延伸閱讀

什麼是異地備援？

「異地備援」的意思是：把重要的資料或系統，備份一份到別的地方。就像把重要文件（比如戶口名簿、存摺），不只放在家裡，也放一份在老家或保險箱裡。這樣如果家裡失火或淹水，資料還有另一份可以用。

為什麼異地備援很重要？

- **防災保命：**如果原本的地方發生火災、地震、水災，備份在別的地方的資料還能用。
- **系統壞了也不怕：**如果主系統壞掉，備援系統可以馬上啟動，不中斷服務。
- **提高安全性：**遇到駭客攻擊或病毒時，備援系統可以幫忙救回資料。
- **快速恢復工作：**不用重建系統，可以快速繼續工作，不會影響公司運作。

小筆記 ：定期檢查備份是否成功（超重要！）

項目	建議頻率	工具建議
檢查備份是否成功	每週 1 次	用 Google 日曆設定提醒
還原測試	每季 1 次	嘗試從備份檔案開啟或復原系統
備份 SOP 教育訓練	每半年 1 次	簡報、流程圖或操作教學影片

附錄｜阿虎百寶箱

可參考的相關資料

行政院公共工程委員會

資訊服務採購評選項目及配分權重範例

組織擇選廠商時，可參考公共工程委員會「資訊服務採購評選項目及配分權重」作為標準，選擇具良好風險管理能力與成本效益之供應商。

資訊服務採購契約範本

與委外廠商訂定合約時，可參考行政院公共工程委員會訂定之「資訊服務採購契約範本」及「資訊雲端服務採購契約範本」。

常用資訊服務等級協議

組織擬定 SLA 時，可參考行政院公共工程委員會 「政府資訊服務採購作業指引」的附件「常用資訊服務等級協議」。

數位發展部資通安全署

委外廠商查核項目表

查核廠商時，可參考數位發展部資通安全署提供之「委外廠商查核項目表」。

常見的資安要求條款

系統設計與開發階段

- **安全設計原則：**系統應依「最小權限原則」與「預設安全原則」進行設計。
- **程式碼安全：**不得使用已知存在漏洞的函式庫、元件，或過時的框架。
- **第三方套件管理：**應定期更新第三方模組，並追蹤其安全性與版本風險。

測試與驗收階段

- **弱點掃描報告：**驗收前須提供弱點掃描結果，並完成高風險項目的修復。
- **滲透測試報告：**高風險系統建議可委由第三方進行滲透測試。
- **驗收標準：**若測試結果未達基本資安要求（例如：無中高等級風險），驗收不予通過。

使用者帳號與存取控管

- **帳號權限控管：**功能需具備角色分級管理，並具有使用行為日誌的功能。
- **預設帳密移除：**系統內不得保留任何預設帳號與密碼。
- **登入安全機制：**應具有密碼強度檢查機制、登入失敗限制與多因子驗證（MFA）。

資料保護

- **加密傳輸與儲存：**網站應全面採用 HTTPS 加密傳輸，對於個資與金流等敏感資料，應使用 AES 等加密技術進行安全儲存。
- **資料存取紀錄：**應記錄所有資料讀取與異動行為，保留完整日誌。
- **不得外傳個資：**明文禁止廠商擅自轉存或洩漏資料至非授權平台或對象。

資安事件應變與責任

- **事件通報時限：**發現資安事件後，廠商應於指定時限內（建議 24 小時）通報。
- **事件調查與補救：**廠商應協助調查、修復並提供完整事故報告。
- **損害賠償機制：**如因廠商疏失造成資料外洩，應承擔法律責任與必要賠償。

專案結束與資料移交

- **資料與程式完整交付：**專案結束時，應交付完整系統原始碼、資料庫結構與操作手冊。
- **資料清除與銷毀：**廠商須刪除其所保留的所有資料，並提供銷毀證明文件。

－結語－

資安路上，您不是一個人

從小雉踏出第一步，到系統順利上線，我們看見了一段真實且熟悉的旅程。委外開發對許多中小企業來說，是節省時間與資源的好方法，但如果忽略了資通安全，省下的成本往往會在事後付出更大的代價。

透過這本《資安星際指南：資通系統安心委外》，我們希望傳達一件事：資安，其實就是一種「多想一步、多問一句、多準備一點」的習慣。

就像小雉一開始也不懂，但他願意學、願意問、願意把「安全」視為系統的一部分而不是附加價值。

資安不是做完就好，而是持續的「照顧」

就像房子住久了，要維修；系統用久了，也要更新、檢查、加強防護。今天跟廠商談好的安全標準，也可能在明天面對新的漏洞與挑戰。

但別擔心，您不是一個人

您可以和廠商一起討論、和團隊一起規劃、和更多經驗者交流。這本手冊，就是您在這條路上的第一本地圖。

最後提醒

每一次委外前，先想想「這次會接觸哪些敏感資料？」
每一份合約中，都能加一句「要做到什麼資安標準？」
每一個驗收，都不忘檢查「安全做到了沒？」
每一次上線之後，也要有「定期檢查與備援」的計畫。

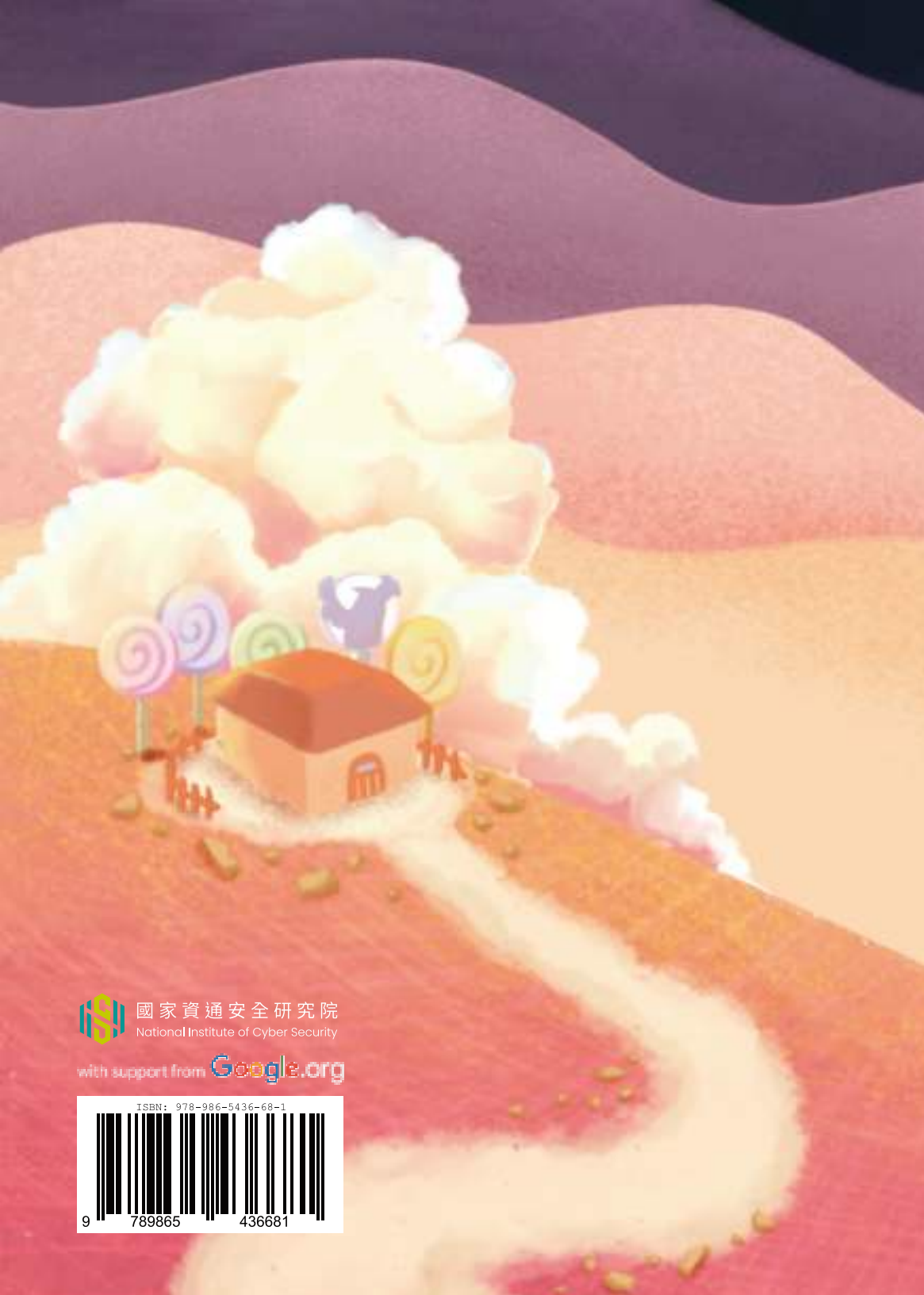
讓我們一起，把資通安全變成日常的一部分，讓每一套系統，不只是好用，更是安心可靠。

因為資通安全不只是技術的事
更是您營運信任的根基

《資安星際指南：資通系統安心委外》

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　鄭瑋
執行編輯　胡馨元
作　　者　邱元貞、張恩鳳、陳思帆
審　　訂　王弘儒、陳奕穎、謝采軒
設　　計　施逸青
出版日期　2025 年 8 月　初版一刷
ISBN　978-986-5436-68-1

本手冊由 Google.org 提供資金挹注「NICS 台灣資安計畫」出版
本手冊由國科會計畫 MOST113-2627-M-002 -001 - 補助



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

with support from Google.org

ISBN: 978-986-5436-68-1