數位發展部數位產業署

資訊服務業
落實個人資料保護暨資訊安全
參考指引

2023 年 12 月

目錄

表目錄

圖目錄

第一章 前言

一、緣起

近年數位技術的發展，個人資料的蒐集、處理或利用方式，逐漸從傳統的紙本形式轉變為電子檔案形式，以及利用網際網路為媒介蒐集、處理或利用。使各行各業開始投入數位經濟，例如網路購物、線上訂票、訂房等電子商務服務蓬勃發展，線上公益捐款也成為潮流，這些線上服務都須利用資通系統運作。而資訊服務業（下稱資服業）係提供如上述資訊服務之業者，因此資服業可能蒐集、處理或利用數量龐大的個人資料，隨之伴隨資訊安全事件（消費者、會員個人資料外洩等）及個資侵害風險明顯高於其他產業。但資通系統發生個人資料外洩的成因複雜，但通常不脫資安防護措施的疏漏所致，此時，受客戶委託建置資通系統的資服業者，更需要強化其資訊安全防護措施及個人資料保護安全維護措施。

因此，為了保護消費者、員工、供應商及股東等個人資料，做好資安防護及個人資料安全維護，成為現今從事數位經濟相關產業的企業組織所必須具備的營運條件。數位發展部數位產業署[1]（下稱本署）為使資服業者受電子商務等業者委託提供資訊服務時，能提升個人資料保護管理能力及技術能力，促使資服業者能妥善保護及管理個人資料，並採取技術上及組織上相關的措施，來防止個人資料檔案被竊取、竄改、毀損、滅失或洩漏，特訂定《資訊服務業者落實個人資料保護暨資訊安全參考指引》供資服業者參考。

二、指引內容與說明

（一）適用對象

本指引主要提供參考的對象，為「提供資訊系統服務之資訊服務業者」（行政院主計總處行業統計分類 6312 資料處理、主機及網站代管服務業、620 電腦程式設計、諮詢及相關服務業，以下稱為「資服業者」），資服業者受委託提供資訊系統服務之方式包含建置、維護、維運、代管

[1] 111 年 8 月 24 日行政院院臺規字第 1110184307 號公告，資訊服務及軟體相關產業（582 軟體出版業；620 電腦系統設計服務業；631 入口網站經營、資料處理、網站代管及相關服務業等之網路產業發展及相關部分；639 其他資訊供應服務業(依行政院主計總處行業分類代碼小類及行業名稱)）之主管機關原為經濟部（工業局），自 111 年 8 月 27 日起變更為數位發展部（數位產業署）。

網頁或套裝系統等。例如開店平台系統、企業資源規劃 ERP 系統（Enterprise resource planning System）、飯店物業管理系統（Property Management System）、電子票券平台、捐款平台等。

（二）重要觀念

需特別說明的是，資服業者在遵循個資法相關規範時，除遵循最基礎的個人資料保護法外，尚須遵守所屬中央目的事業主管機關數位發展部所訂定《數位經濟相關產業個人資料檔案安全維護管理辦法》（下稱本部個資安維辦法）。

另外依據個人資料保護法（下稱個資法）第 4 條及個人資料保護法施行細則（下稱個資法施行細則）第 7 條規定，作為受託者的資服業者也需要遵守委託者主管機關訂定之相關法令規範。

（三）透過 PDCA 落實個人資料保護

本指引參考個人資料保護法、個人資料法護法施行細則第 12 條[2]、本部個資安維辦法及國際標準 ISO 27001 資訊安全管理系統、ISO27701 個人資訊管理系統等內容，提出「個人資料檔案安全維護計畫」建議，並包含資訊服務提供者之特有個資保護議題。

1. 透過 PDCA 建立個人資料安全維護計畫

企業組織應採行適當的「個人資料安全維護措施」，防止個資被竊取、竄改、毀損、滅失或洩漏（參個資法第 27 條第 1 項規定）。所謂「適當安全維護措施」，依個資法施行細則第 12 條第 2 項規定，包

[2] 個人資料法護法施行細則第 12 條：「本法...第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。
前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：
一、配置管理之人員及相當資源。
二、界定個人資料之範圍。
三、個人資料之風險評估及管理機制。
四、事故之預防、通報及應變機制。
五、個人資料蒐集、處理及利用之內部管理程序。
六、資料安全管理及人員管理。
七、認知宣導及教育訓練。
八、設備安全管理。
九、資料安全稽核機制。
十、使用紀錄、軌跡資料及證據保存。
十一、個人資料安全維護之整體持續改善。」

含以下措施：一、配置管理之人員及相當資源；二、界定個人資料之範圍；三、個人資料之風險評估及管理機制；四、事故之預防、通報及應變機制；五、個人資料蒐集、處理及利用之內部管理程序；六、資料安全管理及人員管理；七、認知宣導及教育訓練；八、設備安全管理；九、資料安全稽核機制；十、使用紀錄、軌跡資料及證據保存；十一、個人資料安全維護之整體持續改善。

為採行適當的個人資料安全維護措施，資服業者應規劃、訂定及執行一套「個人資料安全維護計畫」(本部個資安維辦法第 3 條參照)。

本指引採用「規劃—實施—檢查—改善」(Plan-Do-Check-Adjust，PDCA）過程模型，引導資服業者建置「個人資料安全維護計畫」，以採行適當的「個人資料安全維護措施」。下圖完整呈現安全維護計畫與 PDCA－規劃、實施、檢查、持續改善等流程結合的架構圖。

圖 1 透過 PDCA 建立個人資料安全維護計畫流程

資料來源：本指引自製

2. 透過 PDCA 識別評估及因應風險

另外，為落實個資保護，資服業者應識別評估及因應各項與個資保護有關之風險。因應風險又包含個資事故發生前、發生時及發生後等因應措施。

PDCA–規劃、實施、檢查、改善流程，亦可用以識別評估及因應風險。

規劃階段，可識別評估風險，包含法規風險（如何遵守自身及業主應適用的法規、遵守契約）、資安建置風險等。

因應風險，則可透過實施、檢查、改善流程，於平時採取維護個資之措施。若不幸發生個資事故，則盡速採取事故應變及補救措施，以及事後矯正改善等措施。

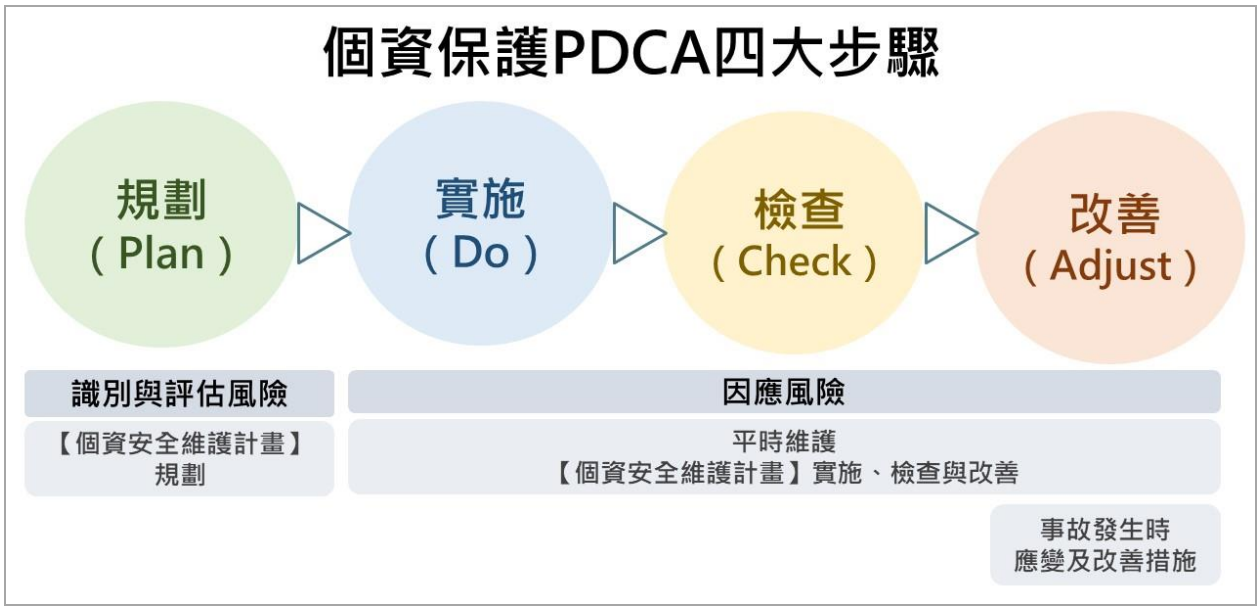


圖 2　個資保護 PDCA 四大步驟

資料來源：本指引自製

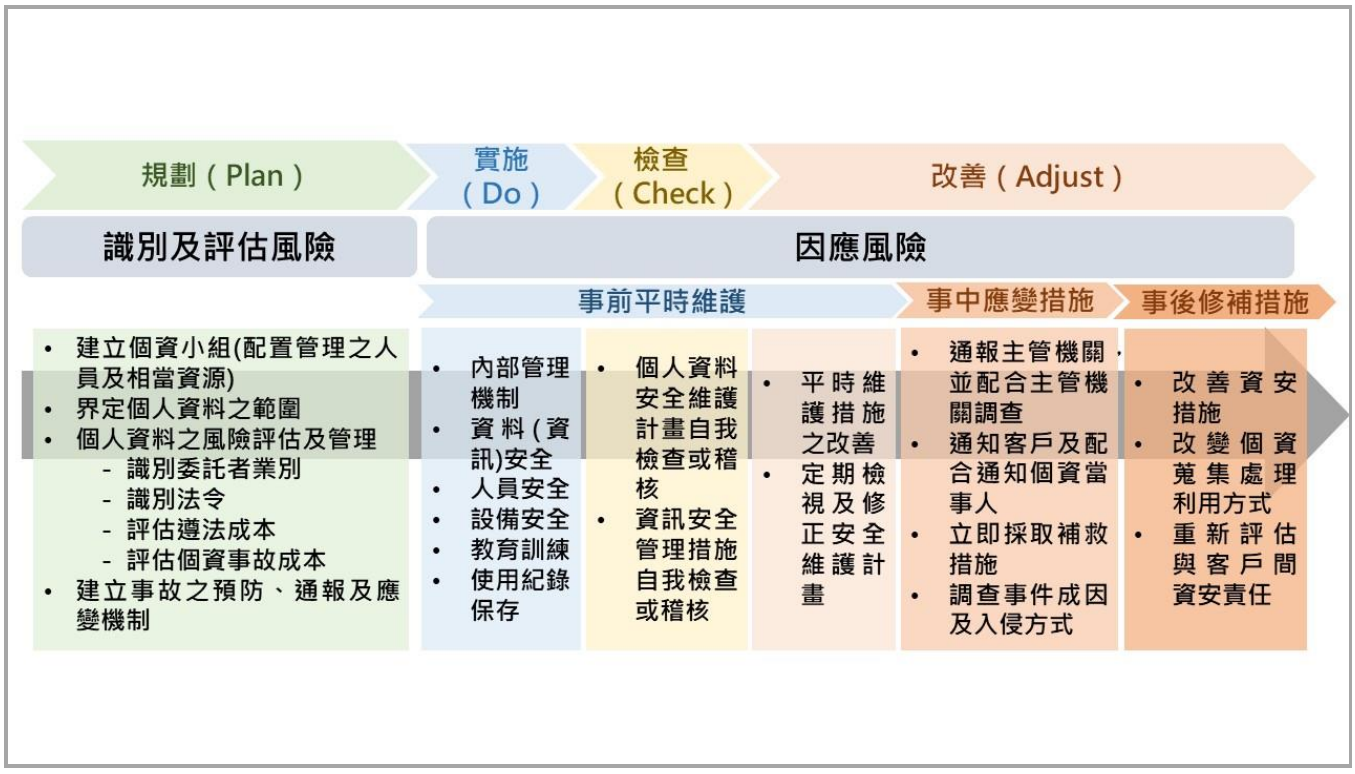


圖 3 透過 PDCA 識別評估及因應風險流程圖
資料來源：本指引自製

三、指引大綱

本指引大綱如下：

第一章:說明編撰資服業者受委託提供資訊系統服務之個人資料保護暨資訊安全參考指引緣起、本指引內容、重要觀念與提醒事項。

第二章：簡介個人資料安全維護計畫之規劃（Plan），包含資服業者可能的委託客戶業別，以及需考量的風險，包含營運風險（個資法令遵法成本、資安要求）及危害風險等。

第三章：簡介個人資料安全維護計畫之實施（Do），就第二章提及之風險，說明事故發生前，平時可採取的維護措施的建構和實作，包含採取個人資料適當安全維護措施及資訊安全管理措施。

第四章：簡介個人資料安全維護計畫之檢查（Check），就第三章的維護措施的建構和實作，進行是否落實的自我檢查或內部稽核，並搭配附錄的「自我檢查表」。

第五章：簡介個人資料安全維護計畫之改善（Adjust），就第四章的檢

查結果進行立刻矯正措施；以及當危害風險（個資事故）不幸發生時，資服業者於事故發生中可採取的應對措施、事故發生後可採取的修補措施，以及需配合主管機關調查。

附錄：提供「資服業者個資安全維護計畫範例」、「業者個人資料蒐集、處理及利用之委外業務監督管理自評表範例」、「資服業者落實個人資料安全維護計畫自我檢查表範例」及「資服業者資訊安全管理措施自我檢查表範例」，供資服業者參考利用。

本署希冀透過本指引，讓資服業者，能對於個人資料管理制度導入與遵循能有更多認知，並且在《個人資料保護法》及相關法規要求的框架下，能以最低的成本和最高的效率完成個資保護措施。

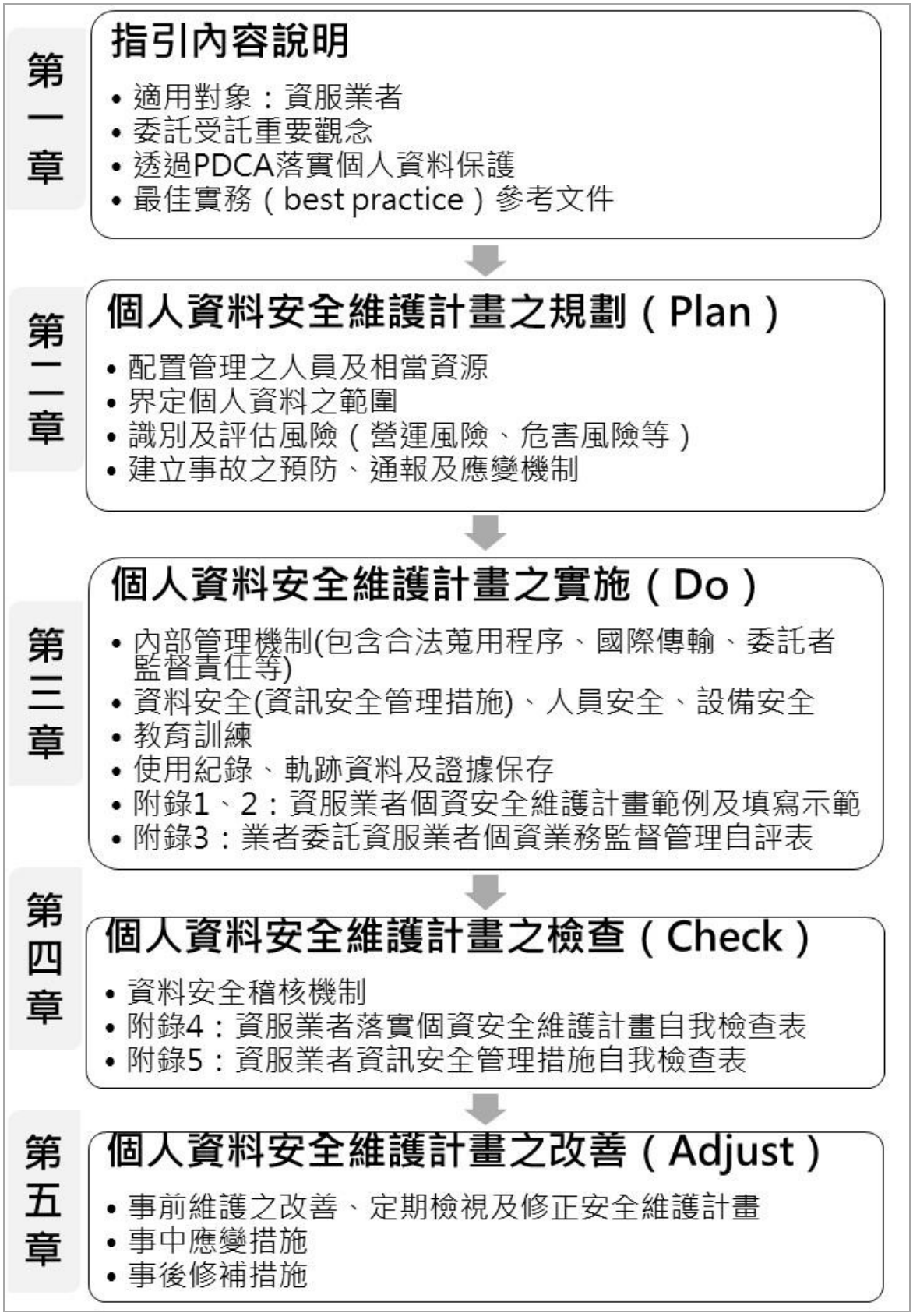


圖 4 指引內容大綱

資料來源：本指引自製

四、最佳實務（best practice）參考文件

規劃、實施、檢查及改善個人資料安全維護計畫時，亦可參考以下個人資訊管理系統與資訊安全管理系統國際標準，以及其他產業主管機關所發布的指引，據以建立企業內部完整的管理制度，以更完整的強化整體個資及資安管理體系。

（一）資訊安全管理系統與個人資訊管理系統國際標準

ISO/IEC 27001 資訊安全管理系統（Information Security Management System）是目前國際上最多企業組織遵循的資訊安全管理系統，企業組織可透過 ISO/IEC 2700 建置符合需求的資訊安全控制措施，以達成一定水準的資安防護能力。[3]

ISO/IEC 27701 個人資訊管理系統(Privacy Information Management System）是建立在 ISO/IEC 27001 之上，在資訊安全擴充及強化個人資料隱私要求和控制措施的管理系統，並整合 ISO 27001、ISO27002、ISO 29100 等實務做法。[4]

（二）臺灣個人資料保護與管理制度（TPIPAS）

「臺灣個人資料保護與管理制度」(Taiwan Personal Information Protection and Administration System，TPIPAS）[5]是我國唯一由政府推動的個人資料管理制度（Personal Information Management System, PIMS），財團法人資訊工業策進會科技法律研究所擔任 TPIPAS 維運機構，由專業團隊負責其維運與持續追蹤國內外隱私保護趨勢接軌。

TPIPAS 的設計是基於我國個資法、OECD、APEC、GDPR 對於個人資料保護要求之重要原則，並結合「個資法遵要求」、「組織管理流程」與「政府認證標章」，從法律面、管理面與程序面確保組織有充分、適當的管理與控制程序，能夠足以符合國內個人資料保護法之最佳法遵實務要求，更有助於達成保護個人資料之目的，組織導入 TPIPAS 可增強

---

[3] ISO/IEC 27701 隱私資訊管理 個人資訊保護的當責與信任，BSI，https://www.bsigroup.com/zh-TW/iso-27701/（最後瀏覽日：2023/08/26）。

[4] ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, ISO, https://www.iso.org/standard/71670.html (last visited Aug. 26, 2023).

[5] 臺灣個人資料保護與管理制度(TPIPAS)，https://www.tpipas.org.tw/（最後瀏覽日：2023/08/26）。

客戶、消費者等利害關係人對於組織個人資料管理能力的信心。

（三）其他業別主管機關參考指引

資服業者受客戶委託提供系統服務，依據個資法第 4 條規定，資服業者受委託而於系統蒐集、處理、利用個人資料時，視同委託者客戶之行為，因此建議資服業者也應參考與遵循委託者客戶所屬產業主管機關訂定之最佳實務參考文件。

所有類型之無店面零售業於 111 年 8 月 27 日前仍全由經濟部商業司（現為經濟部商業發展署）管轄時，經濟部商業司針對無店面零售業之電子商務交易及資訊安全訂有相關指引與參考文件。包含 101 年訂定「電子商務交易安全規範(網路平台、供應商、物流商)修正版」[6]、104 年訂定「電子商務個資外洩資安防護參考指引」[7]、「網路零售資服業者個資防護廠商自評表」[8]、106 年訂定「小型電子商務資服業者資安與個資防護參考指引」[9]（內含「網路零售業資安基本查核表說明」）等參考指引，資服業者可於遵循本指引之餘，亦視委託客戶之屬性參考上述指引。

（四）TWCERT/CC

「台灣電腦網路危機處理暨協調中心（TWCERT/CC）」在數位發展部指導下，協處企業資安事件通報、通報產品資安漏洞、惡意檔案檢測服務，並蒐集及共享國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間的資安情資，以及舉辦資安推廣宣導活動等，其提供之資訊對於提升我國資服業者資安聯防能量及網路安全極有參考價值。

---

[6] 財團法人資訊工業策進會編製，〈電子商務交易安全規範(網路平台、供應商、物流商)修正版〉，經濟部商業司 101 年度電子商務交易安全及資安服務平台推動計畫，101 年 11 月，https://www.cnra.org.tw/edm/ec-cert_1.pdf（最後瀏覽日：2023/08/26）。

[7] 財團法人資訊工業策進會編製，〈電子商務個資外洩資安防護參考指引〉，經濟部商業司 104 年度電子商務交易安全推動計畫，104 年 7 月，https://www.cnra.org.tw/edm/ec-cert_2.pdf（最後瀏覽日：2023/08/26）。

[8] 經濟部商業司，〈網路零售資服業者個資防護廠商自評表〉，104 年，https://gcis.nat.gov.tw/mainNew/matterAction.do?method=showFile&fileNo=t70387_p（最後瀏覽日：2023/08/26）。

[9] 財團法人資訊工業策進會編製，〈小型電子商務資服業者資安與個資防護參考指引〉，經濟部商業司 104 年度電子商務兆元推動計畫，105 年 8 月，https://www.cnra.org.tw/index.php?action=download&cid=160&id=381（最後瀏覽日：2023/08/26）。

因此，鼓勵資服業者至「台灣電腦網路危機處理暨協調中心（TWCERT/CC）」網站首頁[10]，申請加入「台灣 CERT/CSIRT 聯盟」會員，便於接收國內資安事件情資分享，強化資安自我防禦能量。

五、提醒事項

指引內所提示的義務，原則上做為資服業者自我檢視之用。當發生資安事故而致個資侵害時，公司是否違反個人資料保護相關法令，仍宜依照具體事實認定之。

[10] 台灣電腦網路危機處理暨協調中心（TWCERT/CC），https://www.twcert.org.tw/tw/mp-1.html（最後瀏覽日：2023/08/26）。

第二章 個人資料安全維護計畫之規劃（PLAN）

資服業者一開始應規劃建立適當之個人資料安全維護措施。可透過配置管理之人員及相當資源(建立個資小組)、確認委託者之業別、識別及評估營運及危害風險、界定個人資料之範圍、個人資料（設備及蒐用）之風險評估及管理機制、事故之預防、通報及應變機制、，以界定個人資料安全維護措施之實施範圍。

圖 5 個人資料安全維護計畫之規劃（PLAN）
資料來源：本指引自製

一、配置管理之人員及相當資源

個資法施行細則第 12 條第 2 項第 1 款要求資服業者「配置管理之人員及相當資源」。基此，本部個資安維辦法第 5 條規定：「業者應依其業務規模及特性，衡酌經營資源之合理分配，配置管理人員及相當資源，負責下列事項：一、個人資料保護管理政策之訂定及修正。二、安全維護計畫之訂定、修正及執行。（第 1 項）個人資料保護管理政策、安全維護計畫之訂定或修正，應經資服業者之代表人或其授權人員核定。（第 2 項）」

資服業者宜參考上述規定，於安全維護計畫中規劃以下事宜：

（一）配置管理人員及相當資源（成立個資小組）

為落實個人資料保護之目的，資服業者宜考量其業務規模及特性，衡酌經營資源之合理分配，成立個資小組、配置管理人員（一位或以上）及相當資源，負責規劃及推動安全維護計畫及個人資料保護管理政策[11]。

（二）個資管理專員（個資小組總窗口）

管理人員負責訂定個人資料保護管理政策、安全維護計畫，以及辦理個人資料保護法第 27 條所稱之安全維護事項之落實。若組織較為龐大，各部門可皆安排一位個資管理人員。

公司的總管理專員建議以專職為宜（或至少為專責人員），專職的好處在於，除了能最熟悉公司之個資事務外，亦可接受各種外訓，例如 ISO 27001、ISO27701 等國際標準，並進而能成為合格的公司內稽人員。

（三）個資保護總負責人（個資小組召集人）

由於個人資料保護管理政策及安全維護計畫，須有高階管理者之支持，以確保資服業者能確實推動及執行，因此個人資料保護管理政策及安全維護計畫之訂定或修正，應經作為高階管理者之資服業者代表人或其授權人員核定。

基此，公司應有高階管理階層成員擔任個資保護總負責人[12]，其應具統籌各部門之能力，並能提供資源、協調與推動個資保護相關事宜，以利個人資料安全維護事項之運行。並必須檢驗所有資料保護的防護措施部署的執行，並檢驗其是否正確完成。

二、界定及盤點個人資料之範圍

個資法施行細則第 12 條第 2 項第 2 款要求資服業者「界定個人資料之

---

[11] 本部個資安維辦法第 4 條：「資服業者應對內公開周知個人資料保護管理政策，使所屬人員明確瞭解及遵循，其內容應包括下列事項之說明：一、遵守我國個人資料保護相關法令規定。二、以合理安全之方式，於特定目的範圍內，蒐集、處理或利用個人資料。三、以可期待之合理安全水準技術保護其所蒐集、處理或利用之個人資料檔案。四、設置聯絡窗口，供個人資料當事人行使其個人資料相關權利或提出相關申訴與諮詢。五、規劃緊急應變程序，以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。六、如委託蒐集、處理或利用個人資料者，應妥善監督受託者。七、持續維運安全維護計畫之義務，以確保個人資料檔案之安全。」

[12] 所謂由高階管理階層擔任個資保護總負責人，係指由總經理、代表人擔任，或至少副總經理級、法遵長、總稽核，小規模企業由法務長擔任亦可。

範圍」。本部個資安維辦法第 6 條規定：「業者應定期[13]清查確認所蒐集、處理或利用之個人資料現況，界定納入安全維護計畫之範圍。」

因此，資服業者宜參考上述規定，於個人資料檔案安全維護計畫中規劃以下事宜：

（一）蒐集處理利用個人資料之告知

公司要蒐集、處理、利用個人資料時，應對當事人說明個人資料的蒐集、處理及利用之特定目的及特定情形（參見個人資料保護法第 19 條第 1 項各款），以及說明個人資料類別、利用期間、利用地區及利用方式等。之後應將說明內容，寫入個人資料檔案安全維護計畫。

（二）界定個人資料之範圍

公司可能就員工、客戶承辦人、上下游供應商承辦人等的個資，蒐集處理利用。另外，資服業者提供資訊服務時，雖然非未主動蒐集，但受委託傳輸、儲存個資，而有處理個資；或者雖未儲存個資，但建置於客戶端的資訊系統發生故障，資服業者維修時可能接觸儲存在資訊系統內的個資。

個人資料之範圍，包含個人資料保護法第 2 條例示的項目（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），以及其他得以直接或間接識別個人的資料，例如生理資訊、車輛維修紀錄、行車紀錄等。

建議使用法務部訂定之「個人資料保護法之特定目的及個人資料之類別」[14]（包括代號）敘明所蒐集個資之特定目的及類別，例如：「特定目的○○一人身保險」；「個人資料類別 C0 一一 個人描述。例如：年齡、性別、出生年月日、出生地、國籍、聲音等」。

（三）個人資料盤點

蒐集個人資料後，資服業者應進行定期清查盤點，應計算及呈現個

---

[13] 定期之定義參本部個資安維辦法第 18 條。

[14] 個人資料保護法之特定目的及個人資料之類別，國家發展委員會個人資料保護專區，https://pipa.ndc.gov.tw/nc_14773_30638（最後瀏覽日：2023/10/20）。

人資料筆數。此處所謂定期，係指一般資服業者應定期盤點個資，而資本額為新臺幣1000萬元以上或保有個人資料筆數達5000筆以上之資服業者，則應每12個月至少清查盤點及檢討改善一次。(本部個資安維辦法第18條)。

盤點做法沒有特定，雖沒有絕對精準無疏漏的盤點方式，但建議可使用「分析個資流程」方式，盤點出公司所蒐集、處理、利用之個人資料。分析個資流程內容包括下列項目：

- 清查各作業流程中所使用之表單、紀錄，並辨識個人資料有關之表單、紀錄，歸納整理成個人資料檔案。
- 使用個人資料盤點表檢視其保有之個人資料檔案，確認個人資料檔案名稱、保有之依據及特定目的、個人資料種類。

使用個人資料盤點表檢視其保有之個人資料檔案之生命週期及其適法性，包含蒐集、處理、利用之過程及是否合法。

三、個人資料之風險評估及管理機制

資服業者在接受客戶委託提供資訊服務前，需識別及考量與個人資料保護有關的措施，以進行後續的風險評估。綜觀目前企業採取個人資料保護有關之作為時，主要有營運風險（包含遵法成本與資安要求）及危害風險（包含蒐集、處理及利用個資之流程及設備）兩大項重點需做考量。

另外，可將識別風險的結果，以及評估後擬採取或已採取措施，製作風險評估結果清冊等文件化工作。

（一）確認委託者之業別

資服業者依據個資法第4條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」、個資法施行細則第7條：「受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。」，資服業者受委託建置系統，資服業者而於系統蒐集、處理、利用個人資料時，視同委託者之行為，並遵守委託者主管機關之相關法令規範及常見的最佳實務。因此，資服業者需要確認委託者的業別。

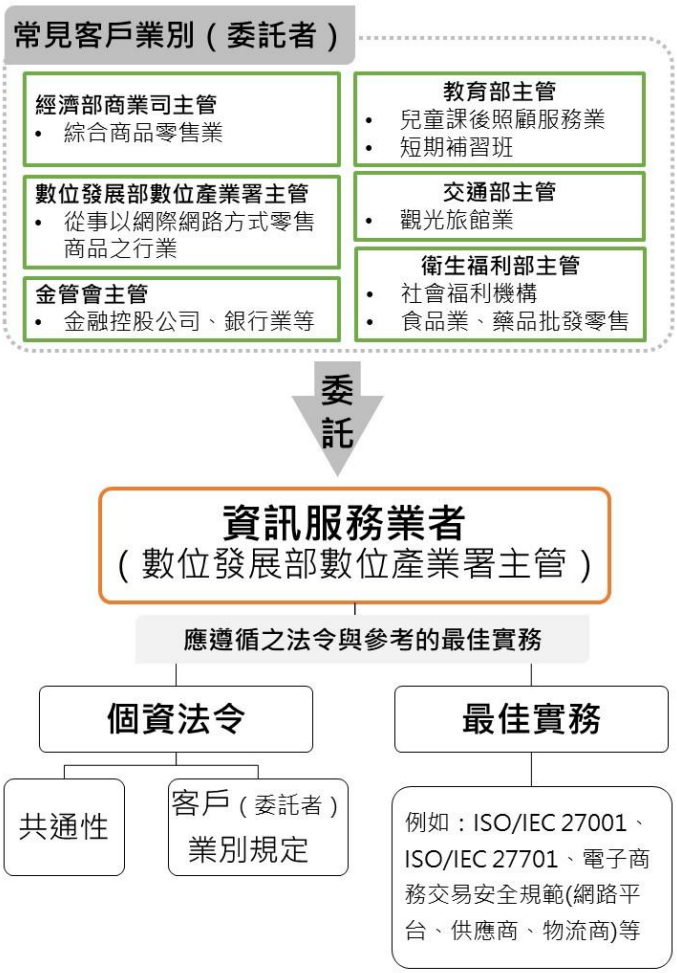


圖 6 確認委託者之業別並遵循個資法令及參考文件
資料來源：本指引自製

基於上述，以下將介紹資服業者需分析與評估各項風險，風險包含須注意的營運風險（法令要求、資安要求）及危害風險（個資事故）。

（二）營運風險：法令要求之遵法成本

個資相關法規範對於資服業者的個資安全維護要求，資服業者須將之納入事業經營的重要考量，若不加以重視，無法投入相應資金及人力等成本遵循相關要求，則可能產生個資事故之風險，例如個資不當蒐集、處理、利用，或者個資外洩。

資服業者在遵循個資法相關規範時，應遵循最基礎的個人資料保護法、個人資料保護法施行細則、本部個資安維辦法，以及依據個資法第4條即個資法施行細則第7條規定遵守委託者主管機關訂定之相關法令規範。

1. 個人資料保護法及個人資料保護法施行細則

個人資料保護法的規範對象主要以「公務機關」與「非公務機關」兩大類來區分。

「非公務機關」係指公務機關以外的「自然人」、「法人」或其他團體（個資法第 2 條第 8 款），因此不論是個人、公司、民間團體都適用於個資法。此外，個資法並沒有設置適用門檻，亦即即使公司只保有 1 筆個資，一樣需要適用個資法相關規定。而所謂 1 筆，是指 1 個自然人的個資而言。

另外，個人資料保護法第 27 條規定，保有個人資料的企業組織，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關則可以指定非公務機關訂定「個人資料檔案安全維護計畫」及「業務終止後個人資料處理方法」。

個人資料保護法施行細則係就個人資料保護法部分條文的細部作法，訂有較詳細的規定。例如就個人資料保護法第 27 條所稱「適當之安全措施」，施行細則於第 12 條規定 11 款措施事項。

2. 行政院建議之資料安全管理措施

依據「行政院及所屬各機關落實個人資料保護聯繫作業要點」（112 年 5 月 29 日修正）第 5 點規定，為強化資安標準規範，保有消費者交易、使用商品或接受服務等過程之一般或特種個資，且符合中央目的事業主管機關所定應加強管理之條件（如：個資數量、該資服業者資本額達一定金額或其他中央目的事業主管機關指定之特定標準）者，應至少訂定下列資料安全管理措施：（一）使用者身分確認及保護機制、（二） 個人資料顯示之隱碼機制、（三）網際網路傳輸之安全加密機制、（四）個人資料檔案與資料庫之存取控制與保護監控措施、（五）防止外部網路入侵對策、（六）非法或異常使用行為之監控及因應機制。詳細說明請見下表：

表 1 行政院及所屬各機關落實個人資料保護聯繫作業要點之資料安全管理措施

管制措施	說明
一、使用者身分確認及保護機制	針對資通系統或個資檔案存取，提供使用者識別、鑑別及身分驗證管理機制，如帳密管制、多重認證技術、帳戶鎖定機制、密碼具一定複雜度等。(可參考資通安全責任等級分級辦法附表 10 相關作法)
二、個人資料顯示之隱碼機制	系統呈現介面上，如有個資資訊，應評估使用情境，予以適當且一致性之遮蔽，以為個資保護。
三、網際網路傳輸之安全加密機制	當個人資料進行網路傳輸時，應採用加密機制，包含使用加密傳輸管道、資料加密傳輸等。
四、個人資料檔案及資料庫之存取控制與保護監控措施	針對個人資料檔案及資料庫之儲存，應適當加密；存取時，應提供使用者識別、鑑別及身分驗證管理機制；留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制。
五、防止外部網路入侵對策	針對可能來自於網路的入侵，採取相關的偵測或防護作為，如個人電腦安裝防毒軟體、使用電子郵件過濾機制、設定網路防火牆、架構應用程式防火牆、採用入侵偵測及防禦機制或進階持續性威脅攻擊防禦措施等。
六、非法或異常使用行為之監控及因應機制	針對資通系統或個資檔案之存取，留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制。

資料來源：行政院資安處[15]、行政院及所屬各機關落實個人資料保護聯繫作業要點

[15] 行政院資通安全處，〈強化安維辦法之資安標準規範資通系統之資安防護〉(110/02/03)，頁 15，http://www.parking.org.tw/document/meeting/資料安全管理法及電子商務系統之個資安全維護辦法.pdf （最後瀏覽日：2023/08/26)。

3. 數位經濟相關產業個人資料檔案安全維護管理辦法

數位發展部鑒於所管數位經濟相關產業自行或受委託蒐集、處理或利用大量且重要之個人資料檔案，其所負之安全維護責任應較嚴謹看待，因此為敦促資服業者加強管理及確保個人資料安全維護措施，故依個資法第 27 條第 3 項授權，訂定《數位經濟相關產業個人資料檔案安全維護管理辦法》，具體規範要求業者訂定個人資料檔案安全維護計畫，內容包含配置管理之人員及相當資源、界定及盤點個人資料範圍、風險評估、建立事故之預防、通報及應變機制、建立個人資料內部管理程序、國際傳輸告知義務、資料安全管理、人員安全管理、設備安全管理、認知宣導及教育訓練，以及改善機制等事項。另外也重申個資法有關委託者監督受託者義務，及受託者同時亦應遵循委託者應適用之個資法相關規範。

本部個資安維辦法第 2 至 4 條規定，所有本部所管數位經濟相關產業之資服業者，皆適用本部個資安維辦法，並應訂定個人資料檔案安全維護計畫，及對內公開周知個人資料保護管理政策。另外，本部個資安維辦法第 18 條規定，對於已具有一定業務規模之資服業者（資本額 1000 萬元以上，或保有（蒐集、處理或利用）[16]個人資料筆數 5000 筆以上較多之業者，採取分級管理，強化安全維護措施執行頻率，要求提及「定期」執行之部分安全維護措施應每 12 個月至少執行一次。

[16] 《數位經濟相關產業個人資料檔案安全維護管理辦法》第 18 條說明四。

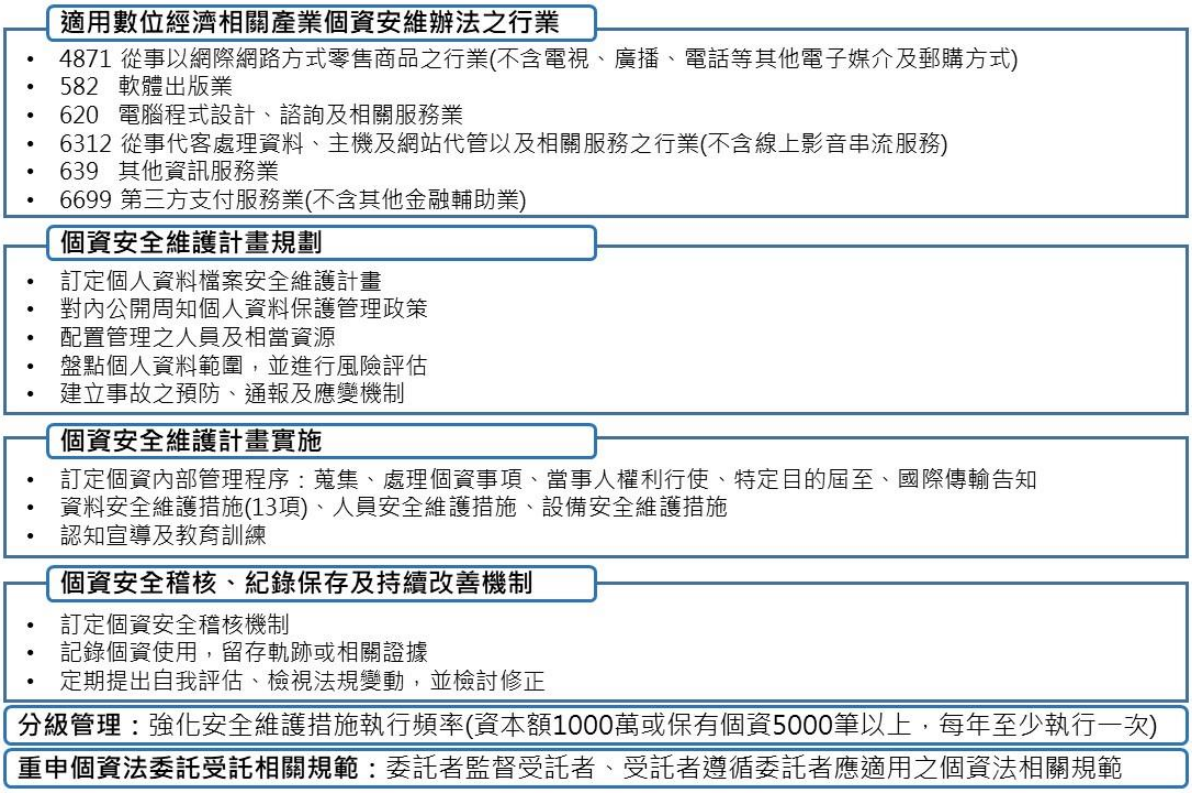


圖 7 數位經濟相關產業個人資料檔案安全維護管理辦法法規架構

資料來源：本指引自製

4. 常見的委託業別相關法規範

個資法第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」，亦即「受託者之個資蒐集、處理或利用行為視為委託者之行為」，由於此時受託者行為已被視為同委託者，因此受託者理應也遵守委託者應適用之法規，個資法施行細則第 7 條因此規定：「受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。」，而本部個資安維辦法第 19 條第 1 項也重申該意旨規定：「業者受委託蒐集、處理或利用個人資料者，應遵循委託者之中央目的事業主管機關所定之個人資料相關法規。」

基此，資服業者應確認委託者之業別，並遵守委託者應適用之相關法令規範，例如依個資法第 27 條第 3 項授權各中央目的事業主管機關訂定之個人資料檔案安全維護計畫或業務終止後個人資料處理方法標準等相關事項之辦法，或其他個人資料相關法規命令。

資服業者常見之委託者（即資服業者之客戶）業別，可能為綜合

商品零售業（線上線下同步）、純以網際網路方式零售商品之行業、食品業、藥品批發零售業、化粧品零售業等（網路購物）；旅宿資服業者（線上訂房）；社會福利機構（線上捐款）；教育服務業、醫院、兒童課後照顧服務業、短期補習班業（會員管理系統）等。以下舉例資服業者常見委託業別之主管機關訂定之「個人資料檔案安全維護辦法」。

(1) 綜合商品零售業

經濟部（商業發展署）依個資法第 27 條第 3 項授權，就綜合商品零售業（主計總處行業代碼 471），訂定《綜合商品零售業個人資料檔案安全維護管理辦法》，該辦法第 3 條規定，從事以非特定專賣形式銷售多種系列商品之零售，已辦理公司、有限合夥或商業設立登記，且資本額達新臺幣 1000 萬元以上，並有招募會員或可取得交易對象個人資料之資服業者，應遵守該辦法之要求。因此受上述綜合商品零售業委託之資服業者亦應遵守該辦法。

(2) 觀光旅館業

就觀光旅館業（營業項目代碼 J901011，主計總處行業代碼 5510），交通部（觀光署）有依個資法第 27 條第 3 項授權訂定《交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法》。

(3) 其他教育服務業

就其他教育服務業（行業代碼 859），教育部亦有依個資法第 27 條第 3 項授權訂定《私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法》（兒童課後照顧服務業，營業項目代碼 JG01011，主計總處行業代碼 8595）、《短期補習班個人資料檔案安全維護計畫實施辦法》（短期補習班業，營業項目代碼 J201031，主計總處行業代碼 8595）等。

(4) 社會福利機構

衛生福利部（社會及家庭署）針對社會福利機構，依個資法第 27 條第 3 項授權訂有《社會福利機構個人資料檔案安全維護計畫實施辦法》，規範以下 3 種類型機構：a.依《私立兒童及少年福利

機構設立許可及管理辦法》之規定，核定之床數逾 95 床之機構；b.依《私立老人福利機構設立許可及管理辦法》之規定，核定之床數逾 200 床之機構；c.依《私立身心障礙福利機構設立許可及管理辦法》之規定，核定之床數逾 200 床之機構。

(5) 食品業

衛生福利部（食品藥物管理署）就食品資服業者，依個資法第 27 條第 3 項授權訂有《食品業個人資料檔案安全維護計畫實施辦法》，規範依《食品安全衛生管理法》第 3 條第 7 款規定，並已辦理公司、商業或工廠登記，且資本額新臺幣 3000 萬元以上，並有招募會員或可取得交易對象個人資料之下列資服業者：a.肉類處理保藏及其製品製造業（主計總處行業代碼 081，限「已屠宰肉類」）；b.磨粉及澱粉製品製造業（主計總處行業代碼 0862、0863）；c.食品及飲料批發業（主計總處行業代碼 454）；d.非屬飯店、觀光旅館、機場或百貨業附屬之餐館業、飲料店業，及非屬餐飲攤販業之其他餐飲業（主計總處行業代碼 561、562、569）。

(6) 化妝品業及醫療器材業

衛生福利部（食品藥物管理署）就醫療器材批發零售資服業者，依個資法第 27 條第 3 項授權訂有《醫療器材批發零售業個人資料檔案安全維護計畫實施辦法》，規範依《醫療器材管理法》第 13 條規定核准登記，且資本額新臺幣 3000 萬元以上，並有招募會員或可取得交易對象個人資料之醫療器材販賣資服業者（主計總處行業代碼 4571、4751）。就化粧品批發零售資服業者，訂有《化粧品批發零售業個人資料檔案安全維護計畫實施辦法》，規範從事化粧品之批發或零售，已辦理公司、商業或有限合夥設立登記，且資本額新臺幣 3000 萬元以上，並有招募會員或可取得交易對象個人資料之資服業者（主計總處行業代碼 4572、 4752）。

(7) 高度監管行業

金融業、醫療業、電信資服業者等主管機關亦屬於高度監理機關，所訂定之個資相關法規範，如《金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法》、《醫院個人資料檔案安全維護計畫實施辦法》、《國家通訊傳播委員會指定非公務機關個人資料檔

案安全維護辦法》等，原則上也會較為嚴格，資服業者受該些業別委託提供資訊系統服務時，應特別評估是否有能力遵循。

(8) 公務機關

資服業者受政府機關、機構及國營事業等委託，建置和營運資訊系統，而該政府機關、機構及國營事業適用《資通安全管理法》時，資服業者應同時注意《資通安全管理法》及相關規範。例如《資通安全事件通報及應變辦法》規定，知悉資通安全事件後，應於 1 小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報，並於 36 小時（第 3、4 級資通安全事件）或 72 小時（第 1、2 級資通安全事件）內完成損害控制或復原作業並通知處理事宜，往後 1 個月內持續進行事件之調查及處理，並送交調查、處理及改善報告。

（三）營運風險：契約與責任分配之遵法成本

資服業者與委託者所訂定的契約，有關個人資料安全維護措施部分，可以在不違反個資法的情況下，訂定雙方的權利及責任分配。

換言之雙方應於締結契約時，即對於資服業者和客戶間的個資安全維護要求，釐清權責分配。而資服業者一旦締約，同樣應將締約內容納入事業經營的重要考量，包含投入資金及人力等成本遵循相關要求，以免產生個資事故之風險時，發現實際上無力遵循。

（四）營運風險：適當個資安全維護措施之要求

近年發生的個資外洩，通常涉及資訊安全問題，為了保護消費者的個人資料，做好資安防護，成為現今從事數位經濟的企業組織所必須具備的營運條件。因此資服業者受委託建置資通系統服務時，自身必須評估其所掌握的資安能力、水準及資金成本，是否足夠防範駭客入侵所產生的個資外洩或其他個資事故。

若是因為資服業者本身的系統漏洞，造成個資外洩等事故發生，則可能被認定未為適當的個人資料安全維護措施，仍可能違反個資法第

27 條規定，而被主管機關依同法第 48 條裁罰[17]。

（五）危害風險：個資事故

近年的個資事故型態，不同於個資法施行早期多為不當蒐集、處理、利用個資事件，現在更多是個資外洩（即洩漏及竊取）事件。資服業者受客戶委託提供資訊服務所使用的資訊系統，也逐漸成為駭客攻擊的主要對象。當資訊服務網頁或資通系統本身有系統漏洞，或資服業者企業內部未防範資安事故，都有可能造成個資外洩事故。

因此，個資法施行細則第 12 條第 2 項第 3 款要求資服業者採取「個人資料之風險評估及管理機制」。本部個資安維辦法第 7 條亦規定：「業者應依已界定之個人資料範圍及其業務涉及個人資料蒐集、處理或利用之流程，定期評估可能產生之風險，並根據風險評估結果，採行適當之安全措施。」

資服業者訂定安全維護計畫時，應先就個人資料進行風險評估，定期評估其已界定之個人資料範圍，及因蒐集、處理或利用個人資料流程中可能面臨之相關風險，以此為基礎建立個人資料風險評估及管理機制，風險評估係識別導致風險之原因，風險管理則在於研擬風險對策。資服業者可參考上述規定，於個人資料檔案安全維護計畫中規劃以下事宜：

1. 風險評估

(1) 系統或設備之風險評估

資服業者應針對內部電腦及內外部資訊系統，以及儲存客戶之消費者個人資料的系統或設備進行盤點，為個人資料可能被竊取、竄改、毀損、滅失或洩漏之風險評估。

(2) 蒐集、處理、利用作業之風險評估

首先將個資類別分為「第 1 級一般」、「第 2 級敏感（財務等）」、「第 3 級特種個資」；以及分類個資屬性為「第 1 級客戶 、供應商

[17] 個資法第 48 條已於 112 年 6 月修正，增訂第 2 項及第 3 項，資服業者若違反個資法第 27 條時，一般案件首次違反立即裁罰並限期改正，裁罰金額為 2 萬至 200 萬，逾期未改正時提高裁罰金額為 15 萬~1500 萬；若屬於情節重大案件，首次即裁罰 15 萬~1500 萬。

及承包商」、「第 2 級所屬人員（員工、業務、兼職、委外、派遣、顧問、股東等）」、「第 3 級消費者」。再將個資類別之數字，加上個資屬性之數字的總合數字，成為評估之「個資檔案價值」。

再者是評估「可能風險類型」，依照資服業者蒐集、處理或利用個資時，產生的各種作業情境及內容，進行個人資料可能被竊取、竄改、毀損、滅失或洩漏之可能風險類型。

作業情境及內容，可能包含加工（例如輸入、編輯、輸出、掃描等）、傳輸（內外部傳輸，可能透過 E-mail、網路伺服器等傳輸）、保管儲存（載體包含個人電腦、資料庫、主機伺服器；風險態樣例如不當存取、個人電腦遭外部攻擊等）、廢棄（例如刪除、資料銷毀不夠落實致外洩）。

最後再依據個資檔案價值評估每個可能風險類型的「風險處理對策」所需投入成本，提出合適的風險處理對策。

(3) 定期評估

一般資服業者應定期評估風險，而資本額為新臺幣 1000 萬元以上或保有個人資料筆數達 5000 筆以上之資服業者，則應每 12 個月至少評估及檢討改善一次（本部個資安維辦法第 18 條）。

2. 風險管理

針對前述個資檔案價值評估及可能風險類型評估之結果，提出預定或已採取之具體風險管理措施或風險處理對策，以及所需投入成本，提出合適的風險處理對策，並製作成「個人資料風險評估表」。

四、事故之預防、通報及應變機制

資服業者應依照前述危害風險之識別及評估內容，訂定個資事故之預防、通報及應變機制。

因此個資法施行細則第 12 條第 2 項第 4 款要求資服業者採取「事故之預防、通報及應變機制」。本部個資安維辦法第 8 條第 1 項也規定，業者為因應當事人個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定應變、通報及預防機制。資服業者可參考以下建議，於個人資料檔案安全維護計畫中規劃事故之預防、通報及應變機制。

（一）事故應變

基於本部個資安維辦法第 8 條第 1 項規定：「一、事故發生後應採取之應變措施，包括降低、控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。」

資服業者應訂定事故應變機制，並建議以流程圖呈現。另外，建議每年至少進行一次事故應變演練，並進行相關檢討。

事故發生時所採取之應變措施，包含發生時、發生後之可能做法或執行流程，例如：

1. 立即通報主管機關

2. 立即通知客戶

3. 協助客戶通知其消費者

4. 立即採取補救措施（尋找惡意程式等）

可透過惡意程式偵測或數位鑑識等方式。若損害層面過大，建議必要時可考慮先將涉及外洩客戶部分之系統伺服器暫停營運（停機）。另外，應採取最基礎的停止損害措施，例如立刻限制國外 IP 存取、限縮客戶帳號存取權限等。

5. 調查事件成因及入侵方式（包含本身系統及網站，以及協助客戶）

調查事件成因之方式，包含調取 log 查閱是否有異常 IP、透過資安健檢尋找後台系統及前台網站漏洞（包含原碼檢測、滲透測試、弱點掃描等）、研究駭客路徑找出其他可能成因（例如員工遭受社交工程攻擊並上當）等。

（二）事故通報

1. 通報主管機關

依本部個資安維辦法第 8 條第 2 項規定：「業者遇有個人資料安全事故，將危及其正常營運或大量當事人權益者，應於知悉事故後七十二小時內依附表二格式通報本部，或通報直轄市、縣（市）政府時副知本部。」資服業者之安全維護計畫應訂定以下通報主管機關內容：

(1) 通報時點：知悉發生事故 72 小時內；若屬重大矚目案件（例如

已被全國性媒體報導[18]），則建議 24 小時內通報。

(2) 通報條件：資服業者遇有個人資料安全事故，將危及其正常營運或大量當事人權益者。

(3) 通報對象：資服業者通報數位發展部，或通報地方政府時副知數位發展部。

(4) 通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法（本部個資安維辦法附表 2[19]、第 8 條第 3 項[20]）。

2. 通知客戶資服業者及協助通知個資當事人

通知當事人部分，理論上應由與消費者直接接觸、蒐集消費者個資之資服業者（例如電商資服業者、飯店民宿、電影院、表演策展單位、私人醫院診所、私立學校、社福機構等），依個人資料保護法相關規定為通知。

不過資服業者與其客戶基於契約關係，協助客戶代管主機或儲存資料時，因而保有消費者個資，因此當知悉消費者個資因資安事故有外洩等情形時，應立即通知客戶資服業者，並可基於與客戶的契約關係，協助客戶資服業者以下事宜：

- 可受客戶資服業者委託，協助代為通知消費者。但通知內容是否合於個資法規定，最終仍應由客戶資服業者自行負責。
- 提醒客戶資服業者通報其主管機關。
- 提供發現事件時立即調查的情形，供客戶資服業者通報主管機關及通知消費者。

---

[18] 所謂重大矚目案件，可參行政院及所屬各機關落實個人資料保護聯繫作業要點（112.05.29）第 2 點第 2 項：「本要點所定重大矚目之個資外洩案件，其範圍如下：(一)行政院、立法院或監察院關注之個資外洩案件。(二)經媒體顯著披露之個資外洩案件，例如經平面媒體全國性版面報導、電子媒體專題討論。」

[19] 本部個資安維辦法附表 2 資服業者個人資料外洩通報表，https://law.moda.gov.tw/Download.ashx?FileID=751 （最後瀏覽日：2023/10/20）。

[20] 本部個資安維辦法第 8 條第 3 項：「無法於時限內通報或無法於當次提供前項所述事項之全部資訊者，應檢附延遲理由或分階段提供。」

以下為《個人資料保護法》第 12 條[21]、《個人資料保護法施行細則》第 22 條[22]、本部個資安維辦法第 8 條第 1 項[23]所規範的適當通知個資當事人方式：

- 通知時點：自知悉時起即應盡速通報。
- 通知條件：資服業者遇有消費者個資被竊取、洩漏（個資外洩）或竄改、損毀、滅失之事故。
- 通知內容：使消費者知悉個資遭外洩或竊取、已採取哪些因應對及修補措施。而非僅是防詐騙宣導。[24]
- 通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。

（三） 事後修補改善措施（事故預防）

事故發生後則進行改善修補措施之方式，降低、控制及預防個資當事人未來再有損害，例如：

1. 改善資安措施

透過已釐清之事件成因進行弱點漏洞修補、部分或全面改善系統資安防護措施等（例如系統架構變更、強化防火牆、傳輸渠道加密、資料庫加密等）。

2. 改變個資蒐集處理利用方式

---

[21] 《個人資料保護法》第 12 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

[22] 《個人資料保護法施行細則》第 22 條：「本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。（第 1 項）依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。（第 2 項）」

[23] 本部個資安維辦法第 8 條第 1 項：「...二、適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式，通知當事人事故之發生與處理情形，及後續供當事人查詢之電話專線或其他適當管道。...」

[24] 行政院院臺訴字第 1100168370 號訴願決定書意旨略以：「...非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人，通知當事人之內容需應包括個人資料被侵害之事實及已採取之因應措施，若該等內容僅係防詐騙提醒，並無會員個人資料被侵害之事實及已採取之因應措施，難認非公務機關已踐行法定通知義務。」，行政院訴願決定書，https://appeal.ey.gov.tw/File/Decision/07acac3a-665d-4812-baa6-738562a7b303 （最後瀏覽日：2023/10/20）。

包含採取個資最小化措施（例如傳輸個資時遮罩隱碼）、改變個資蒐集內容、改變個資傳輸方式、改變個資儲存地點及方式等。

3. 重新評估與客戶間資安責任

評估客戶是否能承擔改善修補後的資安保護能力成本，重新以契約約定雙方資安責任，或者於客戶無力負擔時不再與該客戶續約，以免使資服業者本身承受過多危害風險。

第三章 個人資料安全維護計畫之實施（DO）

為因應個資事故之危害風險，資服業者應依照前述規劃之個人資料安全維護計畫，於平時實施適當之安全維護措施，包含個人資料蒐集、處理及利用之內部管理程序、資料安全維護措施（資訊安全管理措施）、人員安全維護措施、設備安全維護措施、認知宣導及教育訓練等。

圖 8 個人資料保護暨資訊安全之實施（DO）
資料來源：本指引自製

一、平時實施適當之個資安全維護措施

（一）內部管理程序

本部個資安維辦法第 9 條將個資法中有關個資蒐集、處理或利用之內部管理程序逐一條列，包括檢視是否為特種個人資料、檢視個人資料之蒐集、處理或利用是否符合法定要件、當事人拒絕行銷之處置、當事人行使權利之處理、個人資料正確性之維護、個人資料之刪除等事項。另外，個資國際傳輸之限制、告知及監督，則於本部個資安維辦法第 10 條規範。

因此資服業者可參考本部個資安維辦法第 9、10 條規範，以確保個

人資料之蒐集、處理或利用符合個資法規定。

1. 特種個資法定要件

蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料者，檢視是否符合個資法第 6 條第 1 項但書[25]所定情形。（本部個資安維辦法第 9 條第 1 款）

2. 一般個資蒐集、處理或利用法定要件

(1) 蒐集及處理

檢視適法性：檢視蒐集是否符合個資法第 19 條第 1 項[26]之各項法定依據。（本部個資安維辦法第 9 條第 2 款）

蒐集方式：以何種方式蒐集之個人資料（紙本或電子，電子途徑為官網、APP 或報名表單）。

目的告知：檢視是否符合個資法第 8 條第 1 項或第 9 條第 1 項規定，向當事人告知蒐集之目的，或告知變更使用之目的（本部個資安維辦法第 9 條第 4 款）。或者符合法第 8 條第 2 項或第 9 條第 2 項得免為告知之事由。

是否以符合法規要求方式取得當事人同意：是否依個資法第 7

---

[25] 個資法第 6 條第 1 項：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
一、法律明文規定。
二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。」

[26] 個資法第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害。」

條第 1 項[27]方式取得當事人同意。(本部個資安維辦法第 9 條第 2 款)

最小化原則:個資法第 5 條規定個資蒐集、處理或利用的基本原則:「個人資料之蒐集、處理或利用,.....,不得逾越特定目的之必要範圍,並應與蒐集之目的具有正當合理之關聯。」,亦即應符合「比例原則」(即個資最小化原則),不蒐集非必要、與利用目的無關的個資。

處理方式:以何種方式記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及內外部傳送個資。

(2) 利用

利用個資之適法性:檢視個人資料之利用,是否符合蒐集之特定目的必要範圍。

目的外利用之法律依據:為特定目的外之利用時,如何檢視是否符合個資法第 20 條第 1 項但書[28]所定情形。

目的外利用之同意:經當事人同意而為特定目的外之利用者,如何確保符合個資法第 7 條第 2 項[29]規定。(本部個資安維辦法第 9 條第 3 款)

3. 當事人拒絕行銷之處置

本部個資安維辦法第 9 條第 4 項規定:「資服業者利用個人資料行銷而當事人表示拒絕接受行銷者,確保符合本法第二十條第二項及第三項規定。」個資法第 20 條第 2、3 項規定:「非公務機關依前項規定利用個人資料行銷者,當事人表示拒絕接受行銷時,應即停止利

---

[27] 個資法第 7 條第 1 項:「第十五條第二款及第十九條第一項第五款所稱同意,指當事人經蒐集者告知本法所定應告知事項後,所為允許之意思表示。」

[28] 個資法第 20 條第 1 項但書:「非公務機關對個人資料之利用,除第六條第一項所規定資料外,應於蒐集之特定目的必要範圍內為之。但有下列情形之一者,得為特定目的外之利用:一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要,且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益。」

[29] 個資法第 7 條第 2 項:「第 16 條第 7 款、第 20 條第 1 項第 6 款所稱同意,指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後,單獨所為之意思表示。

用其個人資料行銷。（第 2 項）非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。（第 3 項）」

資服業者應依照前述規範，訂定當事人若拒絕行銷時的後續處理機制，並建議對外公告受理及處理流程圖，使個資當事人知悉。

受理方式應提供當事人免費、快速、容易表達之簡便方式以拒絕接受行銷，例如：免付費電話或簡訊、電子郵件地址、企業網站客戶服務網址、於應用程式（APP）內取消行銷資訊等。

有關拒絕行銷的相關處理方式及注意事項，可參國家發展委員會發布之「拒絕商業行銷指引」[30]。

4. 受理當事人行使權利之程序

(1) 告知義務

個資法第 8 條規定，除有免告知事由，資服業者應對資料當事人踐行告知「當事人依第三條規定得行使之權利及方式」之義務：

A. 告知當事人得依個資法第 3 條規定得行使之權利及方式，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、請求刪除等。

B. 告知當事人得自由選擇提供個人資料時不提供將對其權益之影響。

(2) 受理程序

本部個資安維辦法第 9 條第 6 款規定：「當事人行使本法第三條所定權利之相關事項：（一）提供當事人行使權利之方式。（二）確認當事人或其代理人之身分。（三）檢視是否符合本法第十條但書、第十一條第二項但書及第十一條第三項但書所定得拒絕其請求之事由。（四）依前目規定拒絕當事人行使權利者，應附理由通知當事人。（五）就當事人請求為准駁決定及延長決定期間之程序，

[30] 國家發展委員會，〈拒絕商業行銷指引〉，國發會 112 年 6 月 13 日發法字第 1122001288 號，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzMwL3JlbGZpbGUvNjkyMC8zNzAzNi8zNDUwMDQ5NS1hYzA3LTRlODMtYjcxMy1kNjBkZDgwMjRkMTAucGRm&n=5ouS57WV5ZWG5qWt6KGM6Yq35oyH5byVMTEyMDYxMy5wZGY%3D&icon=..pdf （最後瀏覽日：2023/10/20）。

並應確保符合本法第十三條之規定。（六）當事人請求更正或補充其個人資料者，其應釋明之事項。（七）就當事人查詢、請求閱覽或製給複製本之請求酌收必要成本費用者，應明定其收費標準。」

基此，資服業者應採取措施，確保能完整進行受理當事人行使權利之程序，包含規劃程序並在個人資料安全維護計畫中敘明。以免未確實依照當事人要求處理個資，而不當處理及利用個資，例如當事人已要求刪除個資，但公司未實際刪除，持續利用該當事人個資進行行銷或其他利用。

受理方式至少應與蒐集當事人個資相同之方式、管道、難易度相同，例如若取得個資蒐集同意係在網站或 APP 申請或一鍵同意，則不得要求當事人僅能以寄實體信、傳真或 email 等比原先取得個資複雜之程序請求權利。

資服業者並應使個資當事人知悉當事人行使權利之方式與程序，除文字外，建議提供受理流程圖。

5. 個人資料正確性之維護

本部個資安維辦法第 9 條第 7 款規定：「維護個人資料正確性之機制；個人資料正確性有爭議者，並應確保符合本法第十一條第一項、第二項及第五項規定。」[31]

6. 業務終止後有關於個人資料之處理方式

(1) 特定業務減少或終止

資服業者應訂定有關業務如有減少或其特定業務項目被終止，個人資料處理方法。例如個資刪除之程序及佐證，或個資移轉之原因、對象、方法、時間、地點，以及受移轉對象得保有該個人資料之合法依據。

並踐行個人資料保護法第 9 條所定之告知義務，以使資料當事

[31] 個資法第 11 條：「公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。（第 1 項）個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。（第 2 項）……因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。（第 5 項）」

人知悉其個人資料依契約被移轉至他公司。若當事人不同意移轉，應使當事人能行使個資法第 3 條之權利。

(2) 法人格消滅

資服業者應訂定有關法人格被消滅時個人資料處理方法。例如法人格消滅後如有依契約將個人資料移轉予其他法人之情形，應記錄其原因、對象、方法、時間、地點，以及受移轉對象得保有該個人資料之合法依據。

並踐行個人資料保護法第 9 條所定之告知義務，以使資料當事人知悉其個人資料被移轉至他公司。若當事人不同意移轉，應使當事人能行使個資法第 3 條之權利。

7. 定期檢視特定目的是否已消失或期限已屆滿

資服業者應定期檢視消費者個人資料蒐集之特定目的是否已消失或期限是否已屆滿（本部個資安維辦法第 9 條第 8 款）。此處所稱「定期」，係指一般資服業者應定期檢視，而資本額為新臺幣 1000 萬元以上或保有個人資料筆數達 5000 筆以上之資服業者，則應每 12 個月至少檢視一次。（本部個資安維辦法第 18 條）。

特定目的消失或期限屆滿者，應確保符合個資法第 11 條第 3 項[32]規定。（本部個資安維辦法第 9 條第 8 款）

8. 國際／境外傳輸之限制、告知及監督

本部個資安維辦法第 10 條規定：「業者將個人資料作國際傳輸者，應檢視是否受本部依本法第二十一條[33]所為之限制，並且告知當事人其個人資料所欲國際傳輸之區域，同時對資料接收方為下列事項之監督：一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。二、當事人行使本法第三條所定權利之相關

---

[32] 個資法第 11 條第 3 項：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」

[33] 個資法第 21 條：「非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。」

事項。」

(1) 檢視是否受主管機關限制

資服業者將資料傳輸到位在我國以外國家地區之伺服器或資料庫，則有個人資料為國際／境外傳輸之情形。此時資服業者應檢視傳輸區域是否受本部限制。（個資法第 21 條）

(2) 告知「個資有國際／境外傳輸」義務

本部個資安維辦法第 10 條規定有國際／境外傳輸情形者，業者應踐行告知資料當事人，其個人資料會傳輸至我國以外地區，並進行處理、利用，使我國的資料當事人得以知悉個人資料之利用地區將不限於我國境內。

此處規定之業者，係指直接面對消費者並蒐集其個資之業者，例如僅從事以網際網路方式零售商品之業者、線上遊戲軟體出版業者、第三方支付服務業者等。

至於資服業者通常係受前述業者委託蒐集、處理或利用資料，非直接面對消費者之一方，因此資服業者非向消費者為傳輸區域之告知，而係向委託者為傳輸區域之告知，以利委託者依前項規定告知個人資料當事人。

（二）資料安全管理措施

個資法施行細則第 12 條第 2 項第 6 款規定業者應採取「資料安全管理及人員管理」，因此本部個資安維辦法第 11 條訂有資料安全維護措施。本指引以下參考法規要求給予安全維護計畫內容之建議，其他技術層面內容請詳見本指引之【資訊安全管理措施】部分。

1. 一般資料安全管理措施

業者蒐集、處理或利用個人資料檔案者，應依據個人資料風險評估之結果，於安全維護計畫中訂定相關資料安全管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。因此本部個資安維辦法第 11 條第 1 項規範以下內容，資服業者應將之納入安全維護計畫：

(1) 資料加密：經風險評估個人資料有加密之必要者，應於蒐集、處理或利用時，採取適當之加密措施。

(2) 資料備份：經風險評估個人資料有備份之必要者，應對備份資料採取適當之保護措施。

(3) 傳輸安全：傳輸個人資料時，應依不同傳輸方式及其風險評估結果，採取適當之安全措施。

2. 資通系統之資料安全管理措施

資服業者以資通系統直接或間接蒐集、處理或利用個資時，除了採取前述一般資料安全管理措施外，也應採取資通系統之適當管理措施，本部個資安維辦法第 11 條第 2 項規範以下內容，資服業者應將之納入安全維護計畫：

(1) 外部網路入侵對策：建置防火牆、電子郵件過濾機制或其他入侵偵測設備（例如端點防護）等防止外部網路入侵對策，並定期更新。

(2) 異常存取資料行為之監控及因應演練：資通系統存有個資者，應設定異常存取資料行為之監控及定期演練因應機制。

(3) 檢測系統漏洞及修補：確認蒐集、處理或利用個資之電腦、相關設備或系統具備必要之安全性，採取適當之安全機制，定期檢測並因應系統漏洞所造成之威脅[34]。

(4) 防毒軟體及惡意程式檢測：與網路相聯之資訊系統存有個人資料者，應隨時更新並執行防毒軟體，及定期執行惡意程式檢測。

(5) 密碼及認證機制：資通系統存有個資者，應設定認證機制，其帳號及密碼須符合一定之複雜度。[35]

(6) 避免利用真實個資測試：處理個資之資通系統進行測試時，應避免使用真實個資；使用真實個資者，應訂定使用規範。

(7) 資訊系統變更：處理個資之資通系統有變更時，應確保其安全性未降低。

---

[34] 本指引建議，檢測方式至少包含：系統建置時之源碼掃描、網站弱點掃描、系統主機弱點掃描、系統主機滲透測試等。弱點掃描應確保不具有中風險及高風險漏洞。

[35] 本指引建議資服業者提供給委託者之資通系統服務，其認證機制應至少採取雙因子認證，不宜僅以帳密作為唯一登入系統之認證機制，以防帳密外洩時，不會被不明人士以合法登入方式登入系統竊取資料。

(8) 定期檢查資通系統情形：定期檢視處理個資之資通系統，檢查其使用狀況及存取個資之情形。

(9) 個資隱碼：評估使用情境，採行個資之隱碼機制，就個資之呈現予以適當且一致性之遮蔽。[36]

(10) 其他資料安全管理措施：資服業者應留意本部是否公告其他資料安全管理措施，以即時符合最新技術之適當安全維護措施要求。

3. 定期執行

上述之「採取防止外部網路入侵對策」、「演練異常存取行為因應機制」、「檢測系統漏洞及修補」、「防毒軟體及惡意程式檢測」及「檢查資通系統使用狀況及存取個資情形」(本部個資安維辦法第 11 條第 2 項第 1~4、8 款)，一般資服業者應定期實施或檢討改善，而資本額為新臺幣 1000 萬元以上或保有個人資料筆數達 5000 筆以上之資服業者，則應每 12 個月至少實施或檢討改善一次。(本部個資安維辦法第 18 條)。

（三）人員安全管理措施

個資法施行細則第 12 條第 2 項第 6 款規定業者應採取「資料安全管理及人員管理」，因此本部個資安維辦法第 12 條訂有人員安全維護措施，資服業者應將之納入安全維護計畫：

1. 保密義務約定

與所屬人員約定保密義務，例如簽署保密協議書。

2. 識別人員

識別業務內容涉及個資蒐集、處理或利用之人員。

3. 人員存取權限之控制

依其業務特性、內容及需求，設定所屬人員接觸個資之權限，並

[36] 所謂「評估使用情境」，舉例如下：1、供企業內部使用之通訊錄，於已採取其他安全維護措施情形下，或可評估不採行隱碼；2、透過 API 傳輸個人資料時，由於外洩風險較大，可評估採行隱碼機制；3、提供電子商務服務時所蒐集之個資為消費者個資，因此建議採行隱碼機制，避免詐騙或詐刷信用卡。

定期檢視其適當性及必要性。例如實體空間人員進出管制措施、系統中共用文件區的存取管制措施等。

所謂定期，係指一般資服業者應就人員存取權限之定期檢視，而資本額為新臺幣1000萬元以上或保有個人資料筆數達5000筆以上之資服業者，則應每12個月至少檢視及檢討改善一次。(本部個資安維辦法第18條)。

4. 人員離退時之資料返還

人員離職時，要求人員返還個人資料之載體，並刪除因執行業務而持有之個人資料。

5. 分散式管理之人員安全管理

本指引提醒，資服業者若採取分散式管理，或沒有固定辦公場所，仍應記錄人員存取、資料返還等管理措施作為執行佐證。

（四）認知宣導及教育訓練

個資法施行細則第12條第2項第7款要求業者實施「認知宣導及教育訓練」，因此資服業者應對內部員工及外部客戶採取認知宣導或教育訓練措施。本部個資安維辦法第13條有訂有相關規範。

1. 內部員工教育訓練

本部個資安維辦法第13條第1項規定：「業者應定期對所屬人員，實施下列個人資料保護認知宣導及教育訓練：一、個人資料保護相關法令之規定。二、所屬人員之責任範圍。三、安全維護計畫各項管理程序、機制及措施之要求。」因此，資服業者應對其所屬員工進行個人資料保護教育訓練，並加強要求員工接受訓練，使所屬人員均能明瞭個人資料保護相關法令之要求、其所負擔之責任範圍及安全維護計畫中各項管理程序、機制及措施之要求。教育訓練應至少包含以下規劃：

(1) 訓練內容

個人資料保護相關法令之規定；所屬人員之責任範圍；本計畫各項管理程序、機制及措施之要求。

(2) 頻率

一般資服業者應定期實施，並敘明實施頻率，例如至少於公司資安或個資政策更新時實施對員工之教育訓練。

而資本額為新臺幣 1000 萬元以上或保有個人資料筆數達 5000 筆以上之資服業者，則應每 12 個月至少實施一次（本部個資安維辦法第 18 條）。

(3) 程序

資服業者應訂定實施頻率，並訂定每次宣導或訓練之主題、議程，且實施簽到、製作會議紀錄、課後評量機制，作為實施之佐證。

2. 內部代表人、負責人及管理人員教育訓練

代表人、負責人或本部個資安維辦法第 5 條規定之個資管理人員，背負組織內推動個資保護及安全維護的重要職責，為使上述人員更明瞭其於安全維護計畫中所擔負之任務及角色，資服業者應依本部個資安維辦法第 13 條第 2 項規定：「對代表人、負責人或第五條所稱管理人員，另應依其於安全維護計畫所擔負之任務及角色，定期實施必要之教育訓練。」

資本額為新臺幣 1000 萬元以上或保有個人資料筆數達 5000 筆以上之資服業者，則應每 12 個月至少實施一次（本部個資安維辦法第 18 條）。

3. 外部客戶認知宣導

雖然本部個資安維辦法第 13 條未要求資服業者對外部客戶進行認知宣導，但本指引仍建議，資服業者宜對其委託者客戶進行個人資料保護認知宣導。

蓋許多委託者客戶為中小型、微型或新創企業，較無個資安全維護能力，須由熟悉資訊服務內容及所採取之個資安全維護措施的資服業者，協助委託者客戶遵守個人資料保護規範及加強管理認知，以配合資服業者之個資安全維護措施，共同維護個人資料安全。

資服業者對其委託者客戶進行認知宣導之內容，建議宣導客戶使用系統時應備有安全環境，例如登入系統之電腦應加裝防毒軟體並定

期掃毒、上傳資料至系統前應先進行惡意程式偵測、應定期進行防範社交工程訓練、不上有資安風險之網站等。另外，也建議於契約中，要求雙方各自應具備的具體個資安全維護措施。

（五）設備安全管理措施

個資法施行細則第 12 條第 2 項第 8 款要求資服業者採行「設備安全管理措施」，本部個資安維辦法第 14 條也訂有相關規定，業者應納入其安全維護計畫：

1. 儲存媒介物

資服業者應依存有個資之儲存媒介物（紙本、光碟片、電腦、自動化機器設備及其他媒介物等）之特性及使用方式，採取適當之設備維護安全管理措施及儲放環境安全管理措施（本部個資安維辦法第 14 條第 1 款）。

2. 人員保管規範

針對所屬人員保管個人資料之儲存媒介物，訂定適當之管理規範（本部個資安維辦法第 14 條第 2 款）。例如設定相關人員之權限以控管其個資存取、定期變更人員識別密碼等。

3. 人員進出管制規範

針對存放儲存媒介物之環境，施以適當之進出管制措施（本部個資安維辦法第 14 條第 3 款）。

4. 過期資料及設備處理措施

資服業者對於過期資料及軟硬體的處理方式應採取措施。例如提供新版本之資料及軟硬體時，應繳回或刪除舊版本。

（六）使用紀錄、軌跡資料及證據保存

個資法施行細則第 12 條第 2 項第 10 款要求資服業者採行「使用紀錄、軌跡資料及證據保存措施」，本部個資安維辦法第 16 條也訂有相關規定，業者應納入其安全維護計畫：

1. 使用紀錄及軌跡資料證據保存

資服業者執行個人資料檔案安全維護計畫時，保存下列紀錄至少

5 年[37]：(1) 個資之蒐集、處理或利用紀錄；(2) 自動化機器設備之軌跡資料；(3) 落實執行個人資料檔案安全維護計畫之證據。

落實個人資料檔案安全維護計畫之證據，係指：(1) 個人資料提供或移轉第三人之紀錄，該紀錄應包括提供或移轉之對象、依據、原因、方法、時間及地點等資訊。(2) 確認個人資料正確性及補充、更正之紀錄。(3) 當事人行使本法第 3 條之權利及處理過程之紀錄。(4) 個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄。(5) 存取個人資料系統之紀錄。(6) 資料備份及確認其有效性之紀錄。(7) 人員權限新增、變動及刪除之紀錄。(8) 因應事故發生所採取行為之紀錄。(9) 定期檢查處理個人資料之資訊系統之紀錄。(10) 認知宣導及教育訓練之紀錄。(11) 稽核及改善安全維護計畫之紀錄。(12) 其他必要紀錄或證據。(本部個資安維辦法第 16 條說明一)

2. 因業務終止而銷毀證據保存

資服業者於業務終止後，亦即因結束業務經營、交易完成、特定目的消失、契約或法令規定期限屆滿等情況，個資蒐集之特定目的消失或期限屆滿。原則上應依個資法第 11 條第 3 項[38]規定刪除、銷毀、停止處理或利用，惟個資當事人往往無從知悉，為避免不必要之糾紛，因此本部個資安維辦法第 16 條第 2 項規定因業務終止而銷毀證據保存之相關規定：業者於業務終止後，其所蒐集、處理或利用之個人資料應依下列方式處理，並留存下列紀錄至少 5 年：

(1) 銷毀

因業務終止而銷毀個人資料者，記錄其方法、時間及地點。

(2) 移轉

---

[37] 本部個資安維辦法第 16 條說明三提及紀錄至少保存 5 年之理由：「鑒於本法（個資法）第 29 條針對業者之損害賠償責任設有推定過失之規定，本部(數位發展部)作為其中央目的事業主管機關，亦得依同法第 22 條規定為行政檢查，或依第 47 條至第 50 條等規定為行政裁罰。為督促業者留存相關文件紀錄，俾利舉證及備供本部檢查，爰參酌本法第 30 條之時效期間，規定相關證明文件紀錄應至少留存 5 年。」

[38] 個資法第 11 條第 3 項：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」

移轉個人資料者，記錄其原因、對象、方法、時間、地點及受移轉對象得保有該個人資料之合法依據。

(3) 其他刪除、停止處理或利用個人資料

其他刪除、停止處理或利用個人資料者，記錄其刪除、停止處理或利用之方法、時間或地點。

（七）安全維護措施執行頻率

雖然本部個資安維辦法第 3 條規定資服業者皆應規劃及訂定符合第 5 條至第 17 條規定內容的安全維護計畫，不過為避免業務規模較小之資服業者負擔過多成本訂定及執行安全維護計畫，因此本部個資安維辦法第 18 條第 1 項規定，資本額為新臺幣 1000 萬元以上或保有個人資料筆數達 5000 筆以上之資服業者，就部分安全維護措施採取執行頻率分級管理，應於安全維護計畫訂定後，每 12 個月至少一次實施及檢討改善相關措施。[39]

部分安全維護措施包含：界定個人資料之範圍（第 6 條）、個人資料之風險評估（第 7 條）、檢視個資蒐集目的是否已消失（第 9 條第 8 款）、部分資料安全管理措施（第 11 條第 2 項第 1 款至第 4 款及第 8 款，包含採取防止外部網路入侵對策、演練異常存取行為因應機制、檢測系統漏洞及修補、更新及執行防毒軟體及檢測惡意程式、檢查資通系統使用狀況及存取個資情形）、檢視個資存取權限（第 12 條第 3 款）、認知宣導及教育訓練（第 13 條第 1、2 項）、資料安全稽核機制（第 15 條），以及檢視安全維護計畫執行狀況及修正計畫（第 17 條第 2 款）。

下表彙整本部個資安維辦法要求各個安全維護措施的執行頻率：

---

[39] 本部個資安維辦法第 18 條其他規範：

1、 業者應開始每 12 個月實施及檢討改善一次之期限：「業者之資本額於本辦法施行後始增資達新臺幣一千萬元以上，或因直接或間接蒐集而保有個人資料達五千筆以上者，應自符合條件之日起六個月後，每十二個月至少實施及檢討改善前項措施一次。（第 2 項）」

2、 資本額定義：「前二項所定資本額，於股份有限公司為實收資本額，於有限公司、無限公司及兩合公司為登記之資本總額，於獨資或合夥方式經營之事業，為登記之資本額。（第 3 項）」

3、 個資筆數增減之認定方式：「因刪除、銷毀或其他方法致保有個人資料筆數減少，且連續二年期間保有個人資料筆數未達五千筆之業者，得不適用第一項規定。但嗣後因直接或間接蒐集而致保有個人資料筆數達五千筆以上者，應於保有筆數達五千筆以上之日起三十日內，恢復適用第一項規定。保有個人資料筆數之計算，以業者單日所保有之個人資料為認定基準。（第 4 項）」

表 2 安全維護措施執行頻率

安全維護措施	執行內容	規模較小之業者	資本額 1000 萬以上或保有個資 5000 筆以上
1.配置管理之人員及相當資源(安維辦法第 5 條)	配置管理之人員及相當資源	隨時	隨時
2.界定個資範圍(安維辦法第 6 條)	盤點(清查)個資檔案及筆數及界定個資範圍	定期	每 12 個月至少 1 次
3.個資風險評估及管理機制(安維辦法第 7 條)	進行風險評估，根據風險評估結果採取適當之安全措施	定期	每 12 個月至少 1 次
4.事故之預防、通報及應變機制(安維辦法第 8 條)	•建立事故預防、通報及應變機制 •事故發生 72 小時內通報	隨時	隨時
5.個資蒐集、處理或利用之內部管理程序(安維辦法第 9 條)	訂有個資內部管理程序	隨時	隨時
	檢視個資蒐集目的是否已消失或期限是否屆滿	定期	每 12 個月至少 1 次
6.國際傳輸限制、告知及監督(安維辦法第 10 條)	•檢視國際傳輸限制 •告知個資當事人國際傳輸區域	隨時	隨時
7.資料安全管理措施(安維辦法第 11 條)	•採取防止外部網路入侵對策 •演練異常存取行為因應機制 •檢測系統漏洞及修補 •更新執行防毒軟體及檢測惡意程式 •檢查資通系統使用狀況及存取情形	定期	每 12 個月至少 1 次

8.人員安全管理措施(安維辦法第 12 條)	檢視個資存取權限	定期	每 12 個月至少 1 次
9.認知宣導及教育訓練(安維辦法第 13 條)	實施教育訓練	定期	每 12 個月
10.設備安全管理措施(安維辦法第 14 條)	•採取個資儲存物保存措施 •採取適當進出管制措施	隨時	隨時
11.資料安全稽核機制(安維辦法第 15 條)	實施個資安全稽核	定期	每 12 個月
12.使用紀錄、軌跡資料及證據保存(安維辦法第 16 條)	保存紀錄至少 5 年	隨時	隨時
13.個人資料安全維護之整體持續改善(安維辦法第 17 條)	持續改善	隨時	隨時
	檢視及修正安維計畫	定期	每 12 個月

資料來源：本指引自製

（八）受託者及委託者應盡義務

鑑於數位經濟相關產業資服業者商業模式多元，可能是委託他人蒐集、處理或利用資料，也可能是受託者，為再次明確個資法關於委託與受託之義務，因此本部個資安維辦法第 19 條明定受託或委託而蒐用資料時應遵循之義務，資服業者於訂定安維計畫時應特別留意。

1. 受託者應遵循委託者適用之法規

依據個資法第 4 條意旨、個資法施行細則第 7 條及本部個資安維辦法第 19 條第 1 項規定，資服業者應遵守委託者主管機關訂定之相關法令規範，已如本指引第二章所述，因此資服業者應於安全維護計畫中，納入相關法規要求之內容。

另外需特別注意的是，若資服業者將受託業務，複委託（再委託）給其他資服業者蒐集、處理或利用個資，複受託者亦應依據上述規範

遵守其委託者及原委託者應適用之規範。(本部個資安維辦法第 19 條說明二[40])。

2. 委託他人蒐集、處理或利用個人資料之管理程序

(1) 監督管理之理由

由於個資法第 4 條規定，受託者蒐集、處理或利用個資之行為視同委託者之行為，因此受託者行為之效果也將歸於委託者。此時委託者無法在將業務委託給他人後即自身事外，因此資服業者有委託他人蒐集、處理、利用個人資料之情形，應對受託者進行個資安全維護之監督管理。盡監督管理責任除了是委託者作為蒐集主體，應盡到保護當事人個資之責任外，也是為了與受託者釐清責任歸屬[41]，亦即若因受託人緣故不幸發生個資事故，委託者可向主管機關證明已盡監督管理之責，並得向受託人求償。

因此個人資料保護法施行細則第 8 條規定：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。(第 1 項)」

(2) 監督管理之方式

個人資料保護法施行細則第 8 條並規定監督內容及方式：「前項監督至少應包含下列事項：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。二、受託者就第十二條第二項採取之措施。三、有複委託者，其約定之受託者。四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。五、委託機關如對受託者有保留指示者，其保留指示之事項。六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個

[40] 本部個資安維辦法第 19 條第 1 項：「資服業者受委託蒐集、處理或利用個人資料者，應遵循委託者之中央目的事業主管機關所定之個人資料相關法規。」說明二：「.....資服業者受委託蒐集、處理或利用個人資料後，又複委託給其他非公務機關蒐集、處理或利用個人資料，該其他非公務機關（即複受託者）除應遵守複委託資服業者（如資訊服務業）之中央目的事業主管機關所定之相關法令規範外，亦應遵循原委託者（如食藥批發零售、旅宿業、社福團體等非公務機關）之中央目的事業主管機關所定之相關法令規範。」

[41] 法務部 101 年 11 月 21 日法律字第 10103107800 號函釋：「受託為個人資料之蒐集、處理或利用者，仍以委託機關為權責歸屬機關。為釐清責任歸屬，委託機關應對受託者為適當之監督，以確保委託處理個人資料之安全管理」。

人資料之刪除。(第 2 項)」

「第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。(第 3 項)」

「受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。(第 4 項)」

本部個資安維辦法第 19 條第 2 項也重申同樣意旨:「資服業者委託他人蒐集、處理或利用個人資料者，應對受託者依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。」

實際作法方面，本指引建議：資服業者與受託者於契約中敘明個資安全維護責任之事項、請受託者提交資通系統安全檢測之證明、提交安全維護落實情形之自評表[42]及佐證資料，或甚至可對受託者進行稽核 1 年至少 1 次等。

[42] 請見本指引附錄三。

二、資訊安全管理措施

企業組織應於平時，就個人資料管理措施之「資料安全維護措施」，實施「資訊安全管理措施」，強化資安保護措施，以預防資安事故（例如個資外洩）的發生。

平時的資安管理措施，可以從營運管理面、技術防護面、作業流程面、維護、遵循性及持續改善等面向，多方面齊下以防護資安。本指引參考國際標準 ISO/IEC 27001 資訊安全管理系統之內容，提出資訊安全管理措施之執行及政策訂定的建議，並特別包含提供資訊系統服務之特有資安議題。

（一）營運管理面

1. 資訊安全權責

(1) 由高階管理者擔任資訊安全總負責人

資訊安全總負責人可由總經理、代表人擔任、副總經理級或資安長級擔任，即能統籌各部門、協調與推動資安防護相關事宜及所需之資源，且須檢驗所有資訊保護的防護措施的正確完成執行者即可。

(2) 資訊安全總負責人應確保有關資安角色與職權之分配與傳達

明訂與分配組織內部所有資訊安全責任，並確實賦予權利執行。另外，也應注意將相互衝突的職務或責任領域加以區隔。

(3) 資訊安全總負責人應對資安充分支持及承諾

確立保護公司的資訊安全的支持及承諾，將主導組織資安推動的方向，並將有限資源進行最大化發揮及整合，以主導組織資安推動的有效性及效益。例如聘請資安專責人員，或將部分資安維護及健檢事宜外包給資安廠商。

(4) 資訊安全總負責人應對於服務提供之資安給予充分支持

資訊安全總負責人應對服務提供之資安，給予充分支持。資服業者提供資訊服務時，應重視公司客戶的資訊安全，以避免客戶的消費者之個資遭外洩，因此高階管理者，應於公司服務政策中確立，提供安全的資訊服務，是公司服務提供的重要事項，並對於公

司提供資訊服務時，建構資安的資源提供支持。

(5) 高階管理者宜提供資安訓練之資源：

特別留意的是，每位員工若能對於資安觀念正確，認知自己為守護資安的重要一環，將是資安成功的關鍵。因此管理階層宜考量在資安相關訓練的投資，並且教育每位員工瞭解最佳的行事方式及技術知識。

2. 內部營運之資訊安全管理制度

公司應考量營運時所面對的內外部議題，建立一個符合公司目標的資訊安全政策及資訊安全目標，資訊安全政策並應以書面敘明。另外，亦要能識別資訊安全風險並予以對應。

（二）技術防護面

技術防護面分別有「資訊安全作業與保護」、「網路安全防護」、「電腦安全防護」、「資訊系統開發資安防護」、「資料安全管理」、「系統存取控制」、「系統維護」，以及「人員資安認知」等面向，以下分別簡介之：

1. 資訊安全作業與保護

公司應盤點公司的資訊系統，並確立系統作業流程與責任所需之控管方法，以確保資訊處理設施能被正確與安全操作。

實際行動則可透過以下方式執行：

(1) 資訊系統與設備盤點

公司應針對內部電腦及資訊系統，以及儲存客戶之消費者個人資料之系統或設備進行盤點。

(2) 確立系統作業流程的控管方式

系統作業流程可包含涉及變更時之變更控制方法、容量管理、開發測試與運作環境的分隔等。相關控管方法可包含：防範惡意程式的方法、備份以防範資料損失、紀錄系統更新、辨認判斷系統檔案異動之方式、存錄與監控系統檔案異動以記錄事件或留存證據、確保作業系統完整性、防範技術脆弱性等。

2. 網路安全防護

公司應於資訊安全政策文件中敘明為保護網路安全所採取之必要措施，以保護公開網路上的應用服務，並避免詐騙行為、契約爭議及未經授權的存取與修改。

實際行動則可透過以下方式執行：

(1) 建立惡意中繼站黑名單（C2 Server）

利用惡意中繼站黑名單，即可幫助阻擋試圖進入網路的惡意參與者。市面上現有的惡意 IP 黑名單皆可參考利用，包含：行政院技服中心、企業內部蒐集之黑名單、國際即時黑名單列表（RBL）或、DNS 黑名單列表（DNSBL）等。

(2) 網路設備紀錄檔（log）分析

內部對外開放服務連線、內對外連線事件、異常高傳輸量情形、非上班時間之連線情形、內部是否有黑名單連線情形等。

(3) 流量封包側錄

網路封包異常連線、異常 DNS Server 查詢、惡意 IP、內部連接中繼站等符合網路惡意行為的特徵。

(4) 加強縱深防禦

透過資安設備保護內部連線安全，包含安裝 IDS/IPS、WAF、建立 DMZ 緩衝區、垃圾郵件或病毒過濾閘道等。

(5) 企業網段管理

重要系統網段獨立測試、正式環境網段與開發測試網段分離、測試平台禁止真實資料使用。

(6) 定期網頁弱掃、滲透測試

建議至少 1 年進行一次。

3. 電腦安全防護

公司應於資訊安全政策文件中敘明為保護內部電腦安全所採取之必要措施，以防範惡意程式、防範資料損失、確保作業系統完整性、防範技術脆弱性等。

實際行動則可透過以下方式執行：

(1) 關閉未使用服務或具風險之 Port

- 在不影響服務正常運作的情況下，建議 TLS 可升級至最新版，並關閉 TLS 舊版本。
- FTP 應升級為 SFTP，並關閉 FTP。
- Telnet 應升級為 ssh，並關閉 Telnet。

(2) 密碼政策實施

參考國家資通安全研究院標準[43]，系統伺服器密碼應採取強密碼，最少 12 碼；包含英文大寫、英文小寫、阿拉伯數字、特殊符號；密碼更新至少 90 天更新應定期更換密碼，且不可與前 3 次使用過的密碼相同；密碼鎖定原則（密碼輸入錯誤達 5 次後，應至少 15 分鐘內不允許該帳號及來源 IP 繼續嘗試登入，避免遭暴力破解）；建議採用圖形驗證碼機制；密碼重設機制應採取先發送一次性且有時效性的憑證（token），有效回傳後才允許重設密碼。

(3) 建立系統及資料備援

儲存客戶個人資料檔案之媒體與資料，建立備份或備援機制。

(4) 定期主機弱掃、惡意程式檢測

建議至少 1 年進行一次。

(5) 定期軟體更新

定期檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新狀態。

4. 資訊系統開發資安防護

---

[43] 行政院國家資通安全會報技術服務中心，《政府資訊作業委外資安參考指引 v6.3_1110830》，〈附件 3 附錄 1 政府 Web 網站委外安全注意事項與安全檢核表〉，頁 1-9，https://download.nics.nat.gov.tw/UploadFile/attachfilecomm/%E6%94%BF%E5%BA%9C%E8%B3%87%E8%A8%8A%E4%BD%9C%E6%A5%AD%E5%A7%94%E5%A4%96%E8%B3%87%E5%AE%89%E5%8F%83%E8%80%83%E6%8C%87%E5%BC%95v6.3_1110830.rar （最後瀏覽日：2023/10/20）。

傳統程式開發的 SDLC 流程，未將資安考量進去。現在則將資安意識加入，成為 SSDLC 流程作為標準。因此，資訊安全政策文件應特別敘明資訊系統開發之程序與責任，以及相關控管方法，以確保資訊處理設施能被正確與安全操作。

實際行動則可透過以下方式執行：

(1) 設計階段（Design）

於設計階段（Design）考量資安威脅，應分析程式對外服務或內部登入於資安構面是否有風險，須於「威脅建模」(Threat Modeling)逐一列出，並討論解決方式。例如對外網站服務的資安威脅可參考 OWASP TOP 10（十大網路應用系統安全弱點），於設計階段考量資安威脅。

(2) 開發實作階段（Implementation）

應避免常見弱點及發展控制措施。例如：透過 HTTPS 傳輸加密、對稱或非對稱式加密資料庫。

(3) 驗證測試階段（Verification）

包含源碼檢測(靜態分析)、 弱點掃描(動態分析)、滲透測試(動態分析)。

(4) 部署維運階段（Deployment & Maintenance）

透過版本控制工具，掌握版本是否為最新版，並隨時更新版本、修補漏洞，以維持版本的最佳化。

5. 資料安全管理

資服業者對於提供資訊服務，所涉及委託資服業者之客戶的消費者資料，應提出保護資料完整性、機密性及正確性的方法。實際行動則可透過以下方式執行：

(1) 資料傳輸

IT 系統遠端存取連線軟體需升級至企業版本，並將 SQL（結構化查詢語言）更新至最新版，以降低可能存在的資安漏洞。

資服業者透過 API 傳輸個資時，可將個資作有效之加密或隱碼

遮罩，以防不幸發生個資外洩時，減少可被識別的資訊。資服業者透過 API 接受個資時，亦可要求提供個資者將個資最小化，並作有效之加密或隱碼遮罩後再進行傳輸。

(2) 資料庫防護

A.系統內採用加解密機制存取設定資料，並將資料庫、資料表個資採用加解密機制存取資料，並也增設存取 log 紀錄。

B.個資密鑰與資訊系統資料區隔存放於不同位置。

6. 系統存取控制

公司應於資訊安全政策文件中敘明所採取的系統存取控制管理，以防止系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性、完整性及可用性。

實際行動則可透過以下方式執行：

(1) 加強帳號註冊或註銷等權限管理

帳號最低權限原則（嚴格管控）、不共用帳號。

(2) 於系統中布建使用者身分配置程序

(3) 管理使用者密碼資訊及特權存取權限應被限制與管理

(4) 定期檢視使用者權限

隨著內部員工或合約關係（客戶或第三方）的轉變，移除或調整存取權限。

(5) 客戶登入後台之管控

協助客戶強化登入後台資料庫密碼複雜度，並採取多因子認證；限縮有權限進入後台系統（包含下載權限）之人數，但不共用帳密；縮短客戶帳號的登入閒置時間，並於閒置過久時強制登出。

7. 系統維護

(1) 不於非上班時間處理客戶突發問題

以確保所有系統操作皆由公司 IP 進行。

(2) 第三方資安健檢

定期由第三方資安廠商執行資安健檢，並佈署端點防護軟體。

(3) 發現系統弱點列表及控制措施

自主及尋求第三方協助發現的資訊服務系統或網站平台的弱點列表及控制措施，並提出預防或避免攻擊之作法可供線上驗證。

8. 人員資安認知

讓資安成為每一位同仁日常工作中的一環，將是資安成功關鍵。因此公司應透過教育訓練提升員工之資訊安全認知，並於政策文件中敘明資安教育訓練之規劃，包含實施頻率、教育訓練內容（例如：定期更新的組織政策或程序）、及要求員工接受訓練等情形。

實際行動則可透過以下方式執行：

(1) 人員資安職能訓練

可參考政府機關資安職能訓練發展藍圖，透過策略面、管理面、技術面等內容，安排共通訓練、基礎訓練及進階訓練等不同階段的訓練，辦理至少 1 年辦理一次人員資安職能訓練。

(2) 定期電子郵件社交工程演練

每 6 個月至少一次電子郵件社交工程演練，包含收信時不打開可疑信件、瀏覽網頁時不隨意點選可疑連結等，加強員工基本資安意識。

（三）作業流程面

如何做到上述技術面的內容、操作頻率、如何持續操作，就有賴作業流程面的管理。

1. 控制措施

參考 ISO/IEC 27001：2022 資訊安全管理系統之附錄 A，共有 4 大控制主題（組織控制、人員控制、實體控制、技術控制），93 個控制措施。

2. 資訊安全管理的四階文件

可透過以下四階的文件作業，達成作業流程面的管理。

(1) 第一階文件：安全手冊

最高的指導文件在企業資訊安全管理為「安全手冊」內容，包括「資訊安全政策」或國際標準（例如 ISO 27001）之「適用性聲明」等。

(2) 第二階文件：管理辦法

第二階文件是資訊安全的「管理辦法」，將企業資訊安全管理制度文件化。例如：密碼管理辦法。

(3) 第三階文件：作業程序

第三階文件是「作業程序」，規定標準作業細節。例如：密碼轉換及報備作業管理程序、備份作業管理程序、門禁安全作業程序等。

(4) 第四階文件：紀錄表單

最底層的文件是作業流程中實際作業的「紀錄表單」，例如：辦公室安全檢查表、資訊設備攜出表等。

（四）遵循性

檢視個資及資安法令規範，以及於契約上釐清資服業者本身與客戶或第三方之責任，避免違反相關法規（如個資法、客戶之主管機關訂定之相關法規等）及契約義務之要求。

1. 法規要求事項之識別

資服業者應遵守「個人資料保護法」、「個人資料保護法施行細則」、本部個資安維辦法。

另外，由於資服業者係受客戶委託提供資訊系統服務，因此依據個資法第 4 條規定，資服業者受委託而於系統蒐集、處理、利用個人資料時，視同客戶之行為，資服業者因此也需要遵守客戶之主管機關相關法令規範。

2. 契約要求事項之識別

資服業者受委託建置、維運、維護系統，當這些資訊系統發生資安事故時，原因通常多重且複雜，起因有可能發生在資服業者端，也可能來自客戶端，甚至可能發生於租賃第三方的雲端主機。因此對於資服業者，應於訂定契約釐清資服業者本身與客戶或第三方之資安責任，例如下列事項：

(1) 定義所提供 ERP 服務的安全使用環境

於資訊安全文件中敘明資訊服務系統的安全使用環境，應配合採行哪些資訊安全配套措施或工具，以及資料透過 API 傳輸及存取過程之資安防護策略。

(2) 資服業者之委託客戶義務

敘明客戶應備有資訊服務系統的安全使用環境、要求客戶盡資料保護責任。

例如：定期更新各式系統及軟體版本、配合加裝指定之資訊安全配套措施或工具、客戶自建伺服器者之連接加密等級、客戶之電腦設備不可安裝非法軟體、避免多人共用後臺登入之帳密、離開電腦或下班時應從後臺登出、定期且頻繁針對登入後臺的電腦使用防毒軟體掃毒、上傳資料至系統前應就資料進行惡意程式偵測、定期做社交工程教育宣導及演練等。

(3) 資服業者端義務：

敘明資服業者應備有資訊服務系統的安全使用環境，以遵循個人資料保護法要求的個資安全維護措施。

例如：確保網頁安全（SSL 加密）、應設計具加密功能的通道使客戶傳輸機敏資料、應設計傳輸機敏資料時隱碼（遮罩）不必要資訊、得管控客戶存取權限、定期做社交工程教育宣導及演練等。

(4) 租用雲端主機時應釐清責任：

若資服業者或客戶有任何一方，透過第三方資服業者租賃雲端主機或雲端儲存空間者，應在契約中清楚釐清連接架構。並確認哪一方應負擔資料存放和保護管理責任。

（五）證據保存面

公司應落實使用紀錄、軌跡資料及證據等內容的保存，包含以下執行方式：

1. 導入日誌分析系統與事件反應機制

用以作為存錄與監控，以識別、蒐集、獲取及保存可作為證據之資訊，可逐日列舉分析紀錄。

2. 使用紀錄及軌跡資料證據保存

執行資訊安全管理措施時，至少保存以下紀錄：(1) 資料使用紀錄；(2) 自動化機器設備之軌跡資料；(3) 落實執行資訊安全管理措施之證據。

3. 討論紀錄

公司任何優化資安政策程序之討論會議，宜製作書面紀錄以為佐證。

第四章 個人資料安全維護計畫之檢查（CHECK）

本章主要說明事前之平時維護措施之檢查部分。

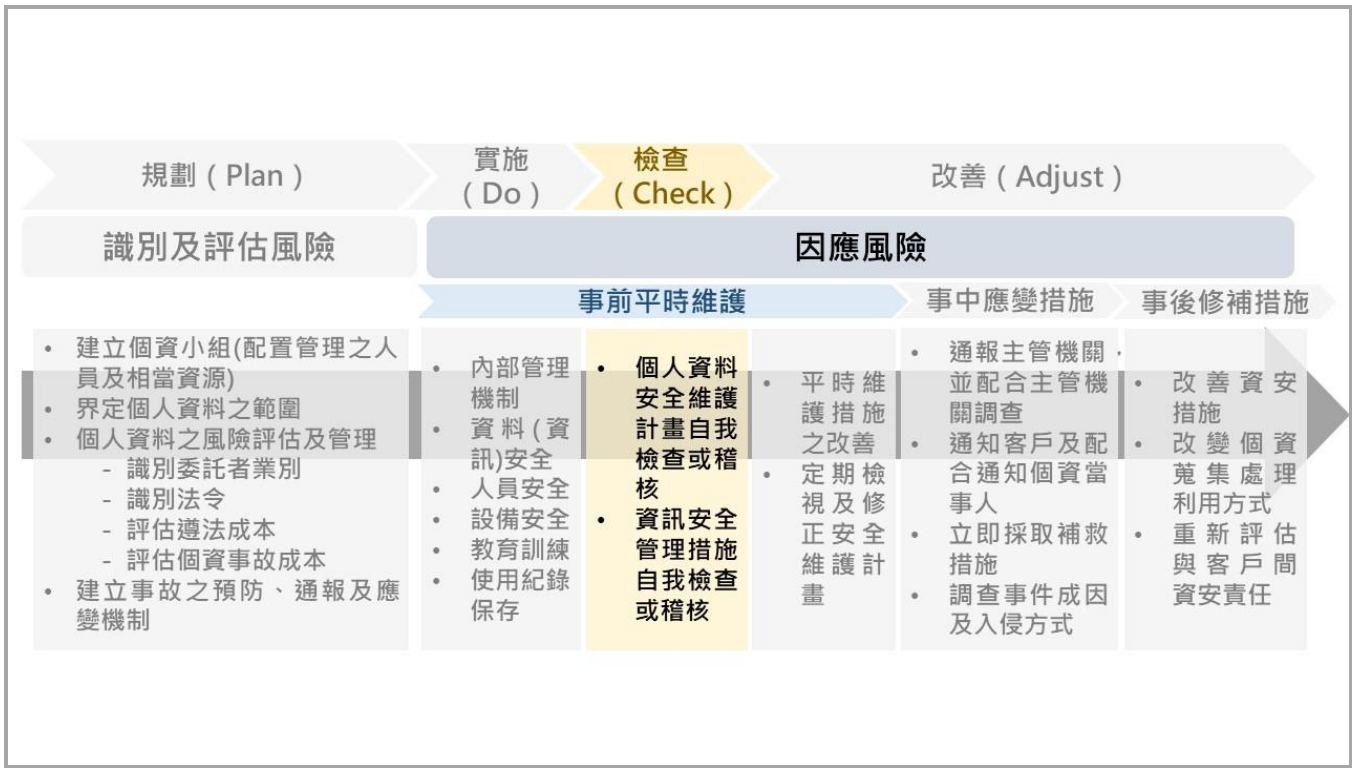


圖 9 個人資料安全維護計畫之檢查（CHECK）
資料來源：本指引自製

個資法施行細則第 12 條第 2 項第 9 款要求業者採行「資料安全稽核機制」，本部個資安維辦法第 15 條亦規定：「業者應訂定個人資料安全稽核機制，定期檢查安全維護計畫執行狀況，並作成評估報告；如有缺失，應予改善。」因此，資服業者應就個人資料保護暨資訊安全平時維護措施的建構和實作等實施內容，定期進行以下檢查措施：

（一）平時自我檢查或內、外部稽核：

1. 自我檢查及內部稽核

資服業者可利用本指引**附錄 4「資服業者落實個人資料安全維護計畫自我檢查表」**，以及**附錄 5「資服業者資訊安全管理措施自我檢查表」**，進行個人資料檔案安全維護及資訊管理管理之平時自我檢查或內部稽核，以檢查執行狀況。

自我檢查或內部稽核頻率，1 年至少 1 次為佳。但資本額為新臺幣 1000 萬元以上或保有個人資料筆數達 5000 筆以上之資服業者，則應每 12 個月至少檢查或內部稽核一次(本部個資安維辦法第 18 條)。

個資專員並應規劃、執行針對全公司進行的自我檢查或內部稽核，並於稽核時紀錄所有過程。若內部稽核人員若取得稽核資格更佳。稽核人員宜由管理、法制及資訊安全之人員擔任之。

2. 外部個資安全稽核機制

若欲展現公司確實具有良好的個資安全維護能力，可進行外部稽核機制，委請第三方驗證機構，依據個資法相關法規及 BS 10012、ISO 27701 等國際標準進行驗證稽核。

資安方面，可委託外部第三方進行資安稽核、資安驗證(例如 ISO 27001)，或委託資安公司進行資安健檢並提出檢測報告。

（二）作成紀錄並回報管理階層審查

資服業者負責自我檢查、內部稽核的人員，或委請的外部稽核人員，應將自我檢查或執行內外部稽核之結果作成評估報告，並依本部個資安維辦法第 16 條第 1 項第 3 款規定保留稽核紀錄。

評估報告也應回報給個資保護及資安總負責人審查。

（三）立即改善及更新個人資料保護暨資訊安全平時維護措施

資服業者應將檢查、稽核等活動發現的缺失立即改善，以及將改善措施內容更新於個人資料安全維護計畫之中。

第五章 個人資料安全維護計畫之改善（ADJUST）

本章說明個人資料安全維護計畫的改善，為因應風險改善的三階段措施，一為事前平時維護程序中，檢查後的改善；另一為當危害風險（個資事故）不幸發生時，資服業者於事中之應變措施，第三為危害風險（個資事故）事後之修補措施。

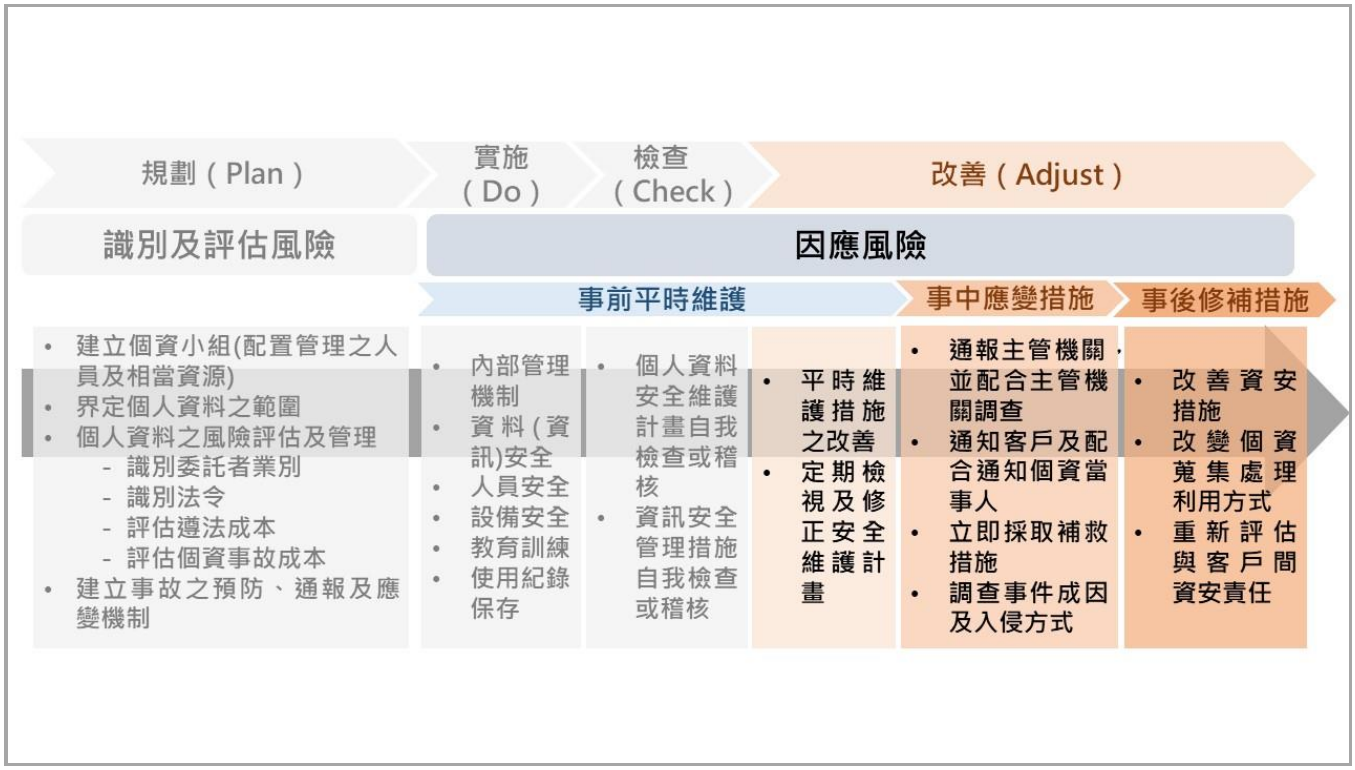


圖 10 個人資料安全維護計畫之改善（ADJUST）
資料來源：本指引自製

一、事前平時維護措施之改善

個資法施行細則第 12 條第 2 項第 11 款要求業者採行「個人資料安全維護之整體持續改善」，本部個資安維辦法第 17 條亦規定：「業者應訂定下列整體持續改善機制：一、安全維護計畫未落實執行時應採取矯正預防措施。二、參酌安全維護計畫執行狀況、技術發展、業務調整及法令變化等因素，定期檢視或修正。」

（一）安全維護計畫未落實執行時應採取矯正預防措施

資服業者於內部自我檢查、內外部稽核等活動中所發現的缺失，宜透過以下方式，採取整體持續改善措施：

- 找出缺失之原因，以及評估是否有類似的缺失存在，或之後可能發生缺失的項目。
- 評估消除缺失項目所須採取的措施，並實際採取該些措施。
- 審查所有已採取的矯正措施的有效性。
- 將矯正措施更新於個人資料安全維護措施及資訊安全管理措施中。
- 將缺失原因、所採取之矯正措施、採取措施的過程、採取措施的結果，皆以文件化方式保存，做為參考依據及證據。

（二）定期檢視及修正個人資料安全維護計畫

參酌安全維護計畫執行狀況、技術發展、業務調整及法令變化等因素，定期檢視或修正。

檢視及修正本計畫，1 年至少 1 次為佳。但資本額為新臺幣 1000 萬元以上或保有個人資料筆數達 5000 筆以上之資服業者，則應每 12 個月至少檢視及修正本計畫一次（本部個資安維辦法第 18 條）。

二、事中應變措施

當資服業者發生個資事故（例如個資外洩）時，應立即進行以下措施：

（一）通報主管機關

依本部個資安維辦法第 8 條規定：

(1) 通報時點：知悉發生事故 72 小時內。

(2) 通報條件：資服業者遇有個人資料安全事故，將危及其正常營運或大量當事人權益者。

(3) 通報對象：資服業者應通報數位發展部（數位產業署），或通報地方政府時副知數位發展部。

(4) 通報方式：為求快速通報，得以 Email 方式通報「數位發展部數位產業署」首長信箱：www-mailbox.adi.gov.tw。

(5) 通報內容：

- 事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因

應措施、通知當事人的時間和方法。

- 第 1 次通報時，不清楚之處可以「不明」、「調查中」撰寫。無法於第 1 次提供之事項及資訊，分階段陸續提供。
- 直接使用本部個資安維辦法附表二[44]。本指引提供通報紀錄表格式範例如下：

表 3 個人資料侵害事故通報與紀錄表

<table>
<tr><th colspan="3">個人資料侵害事故通報與紀錄表</th></tr>
<tr><td>業者名稱
○○○有限公司
通報機關
數位發展部數位產業署</td><td colspan="2">通報時間：○○○年○○月○○日　○○時○○分
通報人：○○○　簽名(蓋章)
職　稱：○○○
電　話：○○○
Email ：○○○
地　址：○○○</td></tr>
<tr><td>事件發生時間
註1：實際發生時間如填寫「不明」者，請接續註明知悉個資外洩之時間</td><td colspan="2">實際發生時間：○○○年○○月○○日 ○○：○○
知悉發生時間：○○○年○○月○○日 ○○：○○</td></tr>
<tr><td rowspan="2">事件發生種類
註2：若為個資外洩，請勾選「竊取」及「洩漏」
註3：尚無法掌握侵害筆數時請寫「目前不明」</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個資侵害之總筆數(大約)
○○○筆</td></tr>
<tr><td>□一般個資 ○○○ 筆
□特種個資 ○○○ 筆</td></tr>
<tr><td>發生原因及事件摘要
註4：請簡要敘述目前掌握的即時情況即可，尚不須填寫詳細確</td><td colspan="2">例：駭客利用境外IP發動攻擊，在系統○○○處植入木馬程式，竊取消費者資料，導致個資外洩</td></tr>
</table>

[44] 數位經濟相關產業個人資料檔案安全維護管理辦法附表二，https://law.moda.gov.tw/Download.ashx?FileID=751 （最後瀏覽日：2023/10/20）。

切原因	
損害狀況 註5：請簡要敘述目前掌握的情況即可	例：○○○年○○月至○○月期間出現多起包含「○○」等○○間客戶網站資料外洩。截至○○○年○○月至○○月止，已掌握○○○筆詐騙通報案
個資侵害可能結果 註6：例如利用個資進行電話詐騙、盜刷信用卡等	例：利用個資進行電話詐騙、盜刷信用卡
擬採取之因應措施 註7：請簡要敘述目前已採取和準備採取之措施即可	例： 1.立即採取補救措施：搜尋及刪除惡意程式、監控後台執行、控管前台風險（阻擋惡意IP、雙因子驗證、建立新的API過濾器）等 2.徹查事件原因：進行資料庫log查詢分析、執行弱點掃描及測透測試找出弱點等 3.協同客戶因應：自○○月○○日起發送事件通知及後續措施予客戶；配合客戶發送通知簡訊及email給消費者 4.擬採取之持續改善措施： (1)變更系統中資料修改權限並加上二次驗證 (2)個人機敏資料遮罩 (3)增加帳號登入密碼定期強迫更新機制
擬採通知當事人之時間及方式 註8：可簡要敘述如何通知客戶；或者如何協助客戶通知客戶之消費者	例：配合電商客戶發送防詐騙簡訊及電子郵件。並協助客戶在其官網及社群網站揭露防詐騙訊息。
是否於發現個資外洩時起算七十二小時內通報 註9：逾72小時通報主管機關者，請簡述延遲通報理由；僅報警者不屬於已通報主管機關	例： □是　　□否，理由：

資料來源：數位經濟相關產業個人資料檔案安全維護管理辦法

（二）通知客戶

資服業者協助客戶代管主機或儲存資料時，因而保有消費者個資，因此當知悉消費者個資因資安事故有外洩等情形時，應基於與客戶的契約關係，先立即通知客戶資服業者。方式不限，能立即、適當、訊息充足，使客戶清楚知悉即可。

另外，應立即要求客戶更新系統、更改密碼、進行惡意程式偵測、弱點掃描、掃毒等。

（三）協助客戶通知其消費者

通報當事人部分，理論上應由與消費者直接接觸、蒐集消費者個資之業者(例如電商資服業者、私人醫院診所、私立學校、非營利組織等)，依個人資料保護法第 12 條規定為通知，不過資服業者可能與客戶基於契約關係，或受客戶另外委託，協助客戶代為通知消費者。

通知消費者的內容，應明確向消費者表示個資遭竊取、已採取的因應措施、通知當事人的時間和方法。若僅寄發提醒防詐騙宣導的內容給遭個資外洩事故之消費者當事人，而未明確向其表示個資已遭外洩，可能會被認為不符個資法第 12 條之規定，而可能會受到個資法第 48 條之處分。[45]應再留意的是，資服業者雖受客戶資服業者委託，協助代為通知消費者，但通知內容是否合於個資法規定，最終仍應由客戶資服業者自行負責。

以下為《個人資料保護法》第 12 條[46]、《個人資料保護法施行細則》第 22 條[47]所規範的適當通知方式：

- 通知時點：自知悉時起即應盡速通報。
- 通知條件：資服業者遇有消費者個資被竊取、洩漏(個資外洩)或竄改、損毀、滅失之事故。

---

[45] 行政院訴願決定書院臺訴字第 1050183642、1050184074 號。

[46] 《個人資料保護法》第 12 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

[47] 《個人資料保護法施行細則》第 22 條：「本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。（第 1 項）依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。（第 2 項）」

- 通知內容：使當事人知悉個資遭竊取、已採取的因應措施、通知當事人的時間和方法。而非僅是防詐騙宣導。
- 通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。

（四）立即採取補救措施

應立即透過惡意程式偵測，或委請資安公司利用數位鑑識等方式，尋找惡意程式（病毒及木馬）並刪除之，立即止血以防止損害擴大。若損害層面過大，建議必要時可考慮先將涉及外洩客戶部分之系統伺服器暫停營運（停機）。

另外，應採取最基礎的停止損害措施，例如立刻限制國外 IP 存取、限縮客戶帳號存取權限等。

（五）調查事件成因及入侵方式

調查事件成因，應調查資服業者提供的資訊系統本身及前台網站，以及協助客戶調查事件成因，並包含客戶委託之第三方資服業者與資服業者所串接的傳輸資訊渠道（如 API 協定等）。

調查事件及入侵方式，包含調取 log 查閱是否有異常 IP、透過資安健檢尋找後台系統及前台網站漏洞（包含原碼檢測、滲透測試、弱點掃描等）、研究駭客路徑找出其他可能成因（例如員工遭受社交工程攻擊並上當）等。

三、事後改善修補措施

當某企業組織發生資安事故（例如個資外洩）後，無論是否已調查出事件成因，都應立即進行以下修補措施：

（一）改善資安措施

若事件已調查出成因，透過已釐清之事件成因進行弱點漏洞修補、部分或全面改善系統資安防護措施等（例如系統架構變更、強化防火牆、傳輸渠道加密、資料庫加密等）。

若尚未調查出成因，針對客戶端的改善，可協助改善資安缺失，例如採取雙（多）因子認證、強制一人一帳戶、限制帳號數、綁定 IP 等。

資服業者系統本身，則應全面建構縱深防禦平台資訊系統的控制措施（例如系統架構變更、強化防火牆、傳輸渠道加密、資料庫加密等），以面對不定期、持續性的網路惡意攻擊。

（二）改變個資蒐集處理利用方式

包含採取個資最小化措施（例如傳輸個資時遮罩隱碼）、改變個資蒐集內容、改變個資傳輸方式、改變個資儲存地點及方式等。

（三）重新評估與客戶間資安責任

評估客戶是否能承擔改善修補後的資安保護能力成本，重新以契約約定雙方資安責任，或者於客戶無力負擔時不再與該客戶續約，以免使資服業者本身承受過多危害風險。

四、配合主管機關調查

依個人資料保護法第 22 條規定，中央目的事業主管機關認有必要或有違反個資法規定之虞時，得請相關人員為必要之說明、配合措施或提供相關證明資料。

數位發展部係資訊服務業之中央目的事業主管機關，於知悉有個資事故發生時，為瞭解所管資服業者與疑似個資外洩事件之關聯，將依前揭規定請資服業者提供相關資料以利釐清問題事件發生之原因。一般於調查時，數位發展部會以發函方式，請資服業者提供說明並備佐證資料，為盡快釐清事故發生成因與責任，建議資服業者於落實各項措施時，應保存相關事證，以於主管機關進行調查時能夠清楚說明。資服業者回函說明及佐證資料大綱如下：

（一）公司資安保護措施

1. 與委託客戶間之關係

- 系統架構圖（例如：系統的網路架構圖、個資傳輸及存放地點架構圖等）及系統架構文字說明。
- 貴公司對客戶之資安環境要求及相關權限控管。
- 貴公司與客戶間之契約要求內容。

2. 事件發生前所採行之平時資料維護措施

（二）個案分析報告

1. 個案分析報告個資外洩發生的可能原因

2. 事件發生時所採取之應變措施

3. 事件發生後所採行之改善措施

另外，為促進國內資安事件情資分享，強化資安防禦體系，提升我國資安自我防護能量，以及使資服業者能即時掌握國內外重大資安事件，建議資服業者加入「台灣 CERT/CSIRT 聯盟」會員。資服業者可至「台灣電腦網路危機處理暨協調中心（TWCERT/CC）」網站首頁[48]，按下「申請加入聯盟」按鈕申請加入會員。

[48] 台灣電腦網路危機處理暨協調中心（TWCERT/CC），https://www.twcert.org.tw/tw/mp-1.html（最後瀏覽日：2023/10/20）。

附錄

附錄 1：資服業者個資安全維護計畫範例

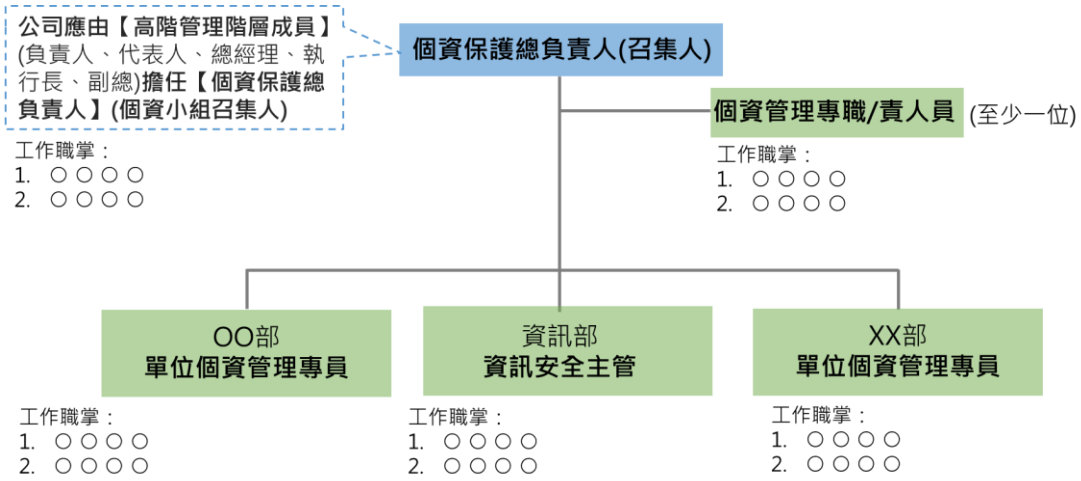
OO 公司個人資料安全維護計畫

OOO 年 OO 月 OO 日 O 版

OO 公司（下稱本公司）依據個人資料保護法、數位經濟相關產業個人資料檔案安全維護管理辦法等相關規範，訂定以下個人資料安全維護計畫(下稱本計畫)，作為本公司個人資料保護管理機制之最高指導文件。

一、個資小組

（註：下圖為參考圖，請業者依實務需求調整內容）



二、個人資料保護管理政策

本公司對內公開周知以下個人資料保護管理政策：

1. 遵守我國個人資料保護相關法令規定。

2. 依照本計畫所列個人資料蒐集、處理及利用之內部管理程序內容，於特定目的範圍內，蒐集、處理或利用個人資料。

3. 依照本計畫所列資料安全管理內容，以可期待之合理安全水準技術保護其

所蒐集、處理或利用之個人資料檔案。

4. 本公司之個資聯絡窗口：

(1) 個資當事人行使其個資相關權利或提出相關申訴與諮詢聯絡窗口：_【註：請填寫專責人員職稱及姓名】

(2) 事故通報個資聯絡窗口：_____【註：請填寫專責人員職稱及姓名】

(3) 緊急應變程序依照本計畫第五點所列之內容進行。

(4) 監督委外廠商依照本計畫第十三點所列內容進行。

(5) 持續維運安全維護計畫之義務，依照本計畫第十五點所列之內容進行以確保個人資料檔案之安全。

三、清查（盤點）及界定個人資料之範圍

（一） 清查（盤點）及界定頻率：_____進行清查（盤點）及界定一次。【註：通常為每半年、每年】

（二） 蒐集、處理或利用個資之屬性

□所屬人員（含員工、業務、兼職、委外、派遣、顧問、股東等人員）

□消費者

□客戶

□供應商、承包商

（三） 個資種類及目的

個資檔案名稱	特定目的	個人資料類別及內容	預計處理或利用方式

【註：使用法務部訂定之「個人資料保護法之特定目的及個人資料之類別」敘明本公司所蒐集個資之特定目的及類別。】

（四） 個資盤點方式

個資檔案名稱	特定目的	個人資料類別及內容	預計處理或利用方式	處理或利用地區	處理或利用期間	資料筆數	建立時間及更新時間	處理及利用軌跡紀錄

【註：透過「個資蒐集、處理及利用流程」盤點個資】

四、個人資料之風險評估及管理機制

（一） 評估頻率：_____進行評估一次。【註：通常為每半年、每年】

（二） 風險評估表

個資檔案名稱	個資類別 1.一般 2.敏感(財務) 3.特種	個資屬性 1.客戶、供應商及承包商 2.所屬人員 3.消費者	個資檔案價值(個資類別+個資屬性)	個資筆數(每月估算)	作業情境及內容	可能風險類型	風險處理對策

【註：先評估「個資檔案價值」(個資類別之數字＋個資屬性之數字的總合數字)及「可能風險類型」，再依據資料價值評估「風險處理對策」投入成本，提出合適的風險處理對策】

（三） 可能風險類型及預訂風險對策

作業情境	作業內容	可能風險類型	預計風險處理對策

【註：提出 5 種作業情境（加工、內部傳輸、外部傳輸、保管、廢棄）的各種可能作業內容（例如加工：輸入/編輯、輸出/列印、掃描），再就各種作業內容預先評估可能的風險類型，並提出預計風險處理對策】

五、事故之預防、通報及應變機制

（一） 事故應變流程圖

「發生個資事故」後，通報個資小組窗口、並由個資小組啟動應變程序，應變程序至少有 3 項，各項應變程序皆完成後始可結案。

1. 事故通報：72 小時內(重大矚目案件 24 小時內)通報主管機關數位發展部並配合調查。
2. 通知當事人：立即通知客戶並配合協助通知當事人，使當事人知悉個資事故及已採取之因應措施。
3. 事故排除及追蹤：立即採取事故排除措施、改善措施、及後續追蹤。

【註：將上述事故應變流程繪製成流程圖】

（二） 事故通報

1. 通報時點：知悉發生事故 72 小時內；若屬重大矚目案件（例如已被全國性媒體報導）24 小時內通報。
2. 通報條件：遇有個人資料安全事故，將危及其正常營運或大量當事人權益。
3. 通報對象：數位發展部。電話：02-23808390；信箱：www-mailbox.adi.gov.tw
4. 通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。（使用數位經濟相關產業個人資料檔案安全維護管理辦法附表二）

https://law.moda.gov.tw/Download.ashx?FileID=751

附表二　業者個人資料外洩通報表

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td>業者名稱

通報機關</td><td colspan="2">通報時間：　年　月　日　時　分
通報人：　　簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td>事件發生種類</td><td>☐竊取
☐洩漏
☐竄改
☐毀損
☐滅失
☐其他侵害事故</td><td>個人資料侵害之總筆數(大約)
_____筆

☐一般個人資料_____筆
☐特種個人資料_____筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料外洩可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於知悉個人資料外洩後72小時通報</td><td colspan="2">☐是　☐否，理由：</td></tr>
</table>

（三） 通知當事人

1. 通知時點：自知悉時起即應盡速通報。
2. 通知條件：遇有個資被竊取、洩漏（個資外洩）或竄改、損毀、滅失之事故。
3. 通知內容：使當事人知悉個資遭外洩或竊取、已採取哪些應對及修補措施。
4. 通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。

六、個人資料蒐集、處理及利用之內部管理程序

（一） 盤點每項個資檔案，確認個資蒐集、處理或利用是否符合法定要件：

1. 特定目的

(1) 利用個資時符合蒐集時之利用目的。

(2) 目的外利用個資，符合個資法第 20 條下列事由：

- 法律明文規定。
- 為增進公共利益所必要，公共利益。
- 為免除當事人之生命、身體、自由或財產上之危險。
- 為防止他人權益之重大危害。
- 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 經當事人同意。(應先告知個資法第 8 條所定應告知事項)
- 有利於當事人權益。
- 特種個資不得目的外利用。

2. 法律依據

(1) 特種個資，符合個資法第 6 條所訂之法律依據

- 法律明文規定。
- 業者履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 當事人自行公開或其他已合法公開之個人資料。
- 學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 經當事人書面同意。(應先告知個資法第 8 條所定應告知事項)【註：但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。】

(2) 一般個資，符合個資法第 19 條之法律依據

- 法律明文規定。
- 與當事人有契約或類似契約之關係，且已採取適當之安全措施。
- 當事人自行公開或其他已合法公開之個人資料。
- 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

- 經當事人同意。(應先告知個資法第 8 條所定應告知事項)
- 為增進公共利益所必要。
- 個資取自於一般可得之來源。【註：但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。】
- 對當事人權益無侵害。

3. 告知當事人

(1) 告知個資當事人，符合個資法第 8、9 條之規定

A.直接向當事人蒐集個資時，明確告知當事人下列事項：

- 業者名稱。
- 蒐集之目的。
- 個人資料之類別。
- 個人資料利用之期間、地區、對象及方式。
- 當事人依第三條規定得行使之權利及方式。
- 當事人得自由選擇提供個資時，不提供將對其權益之影響。

B.蒐集非由當事人提供之個資時，明確告知當事人下列事項：

- 公務機關或非公務機關名稱。
- 蒐集之目的。
- 個人資料之類別。
- 個人資料利用之期間、地區、對象及方式。
- 當事人依第三條規定得行使之權利及方式。

(2) 符合免為告知之情形

A.直接向當事人蒐集個資時符合免為告知之情形

- 依法律規定得免告知。
- 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
- 告知將妨害公務機關執行法定職務。
- 告知將妨害公共利益。
- 當事人明知應告知之內容。

- 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

B. 蒐集非由當事人提供之個資時符合免為告知之情形

- 依法律規定得免告知。
- 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
- 告知將妨害公務機關執行法定職務。
- 告知將妨害公共利益。
- 當事人明知應告知之內容。
- 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。
- 當事人自行公開或其他已合法公開之個人資料。
- 不能向當事人或其法定代理人為告知。
- 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
- 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

4. 最小化原則（比例原則）

蒐集個資時不蒐集與利用目的無關的個資。

5. 國際／境外傳輸之限制、告知

本公司將個人資料作國際傳輸時，將檢視是否受數位發展部依個人資料保護法第 21 條所為之限制，並且告知當事人其個人資料所欲國際傳輸之區域。本公司將對資料接收方為下列事項之監督：一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。二、當事人行使個人資料保護法第 3 條所定權利之相關事項。

（二） 受理當事人請求權利之程序

1. 受理內容

(1) 拒絕行銷之處理程序

(2) 受理當事人行使個資法第 3 條權利之程序

(3) 受理個資更正之程序

2. 拒絕行銷受理方式：

(1) 當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

(2) 首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

(3) 提供當事人免費、快速、容易表達之簡便方式。

3. 當事人行使個資法第 3 條權利受理方式：

(1) 告知當事人得依個資法第 3 條規定得行使之權利及方式

(2) 至少與蒐集當事人個資相同之方式、管道、難易度相同。

(3) 受理後處理方式包含：

- 確認當事人或其代理人之身分。
- 檢視是否符合個資法第 10 條但書、第 11 條第 2 項但書及第 11 條第 3 項但書所定得拒絕其請求之事由。
- 拒絕當事人行使權利者，附理由通知當事人。
- 當事人請求為准駁決定及延長決定期間之程序，並應確保符合個資法第 13 條之規定。
- 當事人請求更正或補充其個人資料者，其應釋明之事項。
- 當事人查詢、請求閱覽或製給複製本之請求酌收必要成本費用者，應明定其收費標準。

4. 個資更正受理方式：

(1) 維護個人資料之正確，並主動或依當事人之請求更正或補充之。

(2) 提供當事人免費、快速、容易表達之簡便方式請求更正或補充之。

(3) 個資正確性有爭議者，應主動或依當事人之請求停止處理或利用。【註：因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。】

(4) 因可歸責於本公司之事由，未為更正或補充之個資，應於更正或補充後，通知曾提供利用之對象。

5. 受理流程圖

【註：依前述內容及公司實際流程繪製。】

七、資料安全管理

本公司之_____系統【註：公司實際提供之資訊服務系統】**、公司 OA 區電腦、共用區設備，採取以下資料安全管理措施：**

1. 加密：儲存於_____【註：公司實際提供之資訊服務系統、共用區設備等】之資料採取_____【註：依公司實際需求，例如 AES256】等加密措施。

2. 備份：備份資料採取_____之保護措施。【註：依公司實際需求，例如加密儲存、自動備份、自動壓縮、自動金鑰加密等】

3. 傳輸安全：_____【註：公司實際提供之資訊服務系統、電子郵件等】之資料透過_____【註：依公司實際需求，例如 API】傳輸時，採取適當_____【註：依公司實際需求，例如 SSL 傳輸加密機制】之安全措施。

4. 外部網路入侵對策：

□建置防火牆：管理系統伺服器及 OA 區網路防火牆只開放必要的通訊埠對外連線，並_____定期更新一次。【註：通常每 3 個月、半年或一年】

□建置應用程式防火牆：網站安裝應用程式防火牆監測、過濾、阻斷可疑的流量，並_____定期更新一次。【註：通常每 3 個月、半年或一年】

□電子郵件過濾機制：員工電子郵件系統採取過濾系統，_____定期更新一次。【註：通常每 3 個月、半年或一年】

□端點防護：OA 區電腦、共用區設備採取端點防護，_____定期更新一次。【註：通常每半年或一年】

□其他入侵偵測設備：_____，並_____定期更新一次。

5. 異常存取資料行為之監控及因應演練：設定異常存取資料行為監控機制；並__定期演練異常存取資料行為因應機制。【註：通常每半年或一年】

6. 檢測系統漏洞及修補：_____【註：通常每半年或一年】定期一次透過__ _____【註：公司實際需要之檢測系統，例如網站弱點掃描、主機弱點掃描或滲透測試】檢測系統漏洞，並修補漏洞至無中風險及高風險漏洞。

7. 防毒軟體及惡意程式檢測：

(1) 設備及系統隨時更新及執行防毒軟體。

(2) _____定期執行惡意程式檢測一次。【註：通常每半年或一年】

8. 密碼及認證機制：

□密碼【註：帳號及密碼須符合一定之複雜度】

□其他認證機制：_____【註：公司實際需求，例如雙因子認證、多因子認證、生物識別等】

9. 避免利用真實個資測試：

(1) 處理個資之資通系統進行測試時避免使用真實個資。

(2) 使用真實個資者，應訂定使用規範。

10. 資訊系統變更：處理個資之資通系統有變更時，應確保其安全性未降低。

11. 定期檢查：_____一次定期檢視處理個資之資通系統，檢查其使用狀況及存取個資之情形。【註：通常每半年或一年】

12. 個資隱碼：針對本公司_____之個資使用情境【註：依公司實際需求，例如 API 傳輸個資、網站前台訂單查詢等】，採行個資之_____隱碼機制。【註：依公司實際需求，例如 SSL 傳輸加密機制、資料顯示之隱碼機制】

13. 其他資料安全措施：_____【註：若有無上述情形，可自行填寫】

八、人員安全管理

1. 保密義務約定：與所屬人員約定保密義務，約定方式：____【註：依公司實際需求，例如簽署保密協議書】

2. 識別人員：識別業務內容涉及個資蒐集、處理或利用之人員。識別方式：＿＿＿＿＿＿。【註：通常依專案內容或業務屬性判斷會蒐用個資的人員】

3. 人員存取權限之控制：依業務特性、內容及需求，設定所屬人員接觸個資之權限，並定期檢視適當性及必要性。

□實體空間人員進出管制措施：＿＿＿＿【註：依公司實際需求，例如辦公室門禁、檔案室門禁、機房門禁】

□系統共用文件區存取管制措施：＿＿＿＿【註：依公司實際需求，例如共用區個別檔案僅該涉及專案之人員才有存取權限】

□其他：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

4. 人員離職時之資料返還程序：＿＿＿＿＿＿＿＿【註：依公司實際需求，例如要求離職人員返還個人資料之載體，並由專責人員進行檢查】

九、設備安全管理

1. 儲存媒介物：依存有個資之儲存媒介物（紙本、光碟片、電腦、自動化機器設備及其他媒介物等）之特性及使用方式，訂有以下管理規範：

□設備維護安全管理措施：＿＿＿＿＿＿【註：依公司實際需求，例如端點防護】

□儲放環境安全管理措施：＿＿＿＿＿＿【註：依公司實際需求，例如檔案室環境規則、共用區存取規則】

□其他：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

2. 人員保管規範：＿＿＿＿＿＿＿＿＿＿【註：依公司實際需求，針對設備保管人訂有定管理規範，例如：該設備存有之資料涉及機密，不得接取可連接外部網路之主機】

3. 人員進出管制規範：＿＿＿＿＿＿＿＿＿＿【註：依公司實際需求，針對存放儲存媒介物之環境，訂有進出管制規範，例如：辦公室門禁、檔案室門禁、機房門禁等措施】

4. 過期資料及設備處理措施：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿【註：依實際需求，對於過期資料及軟硬體的處理方式應採取相應作法，例如：提供新版本之資料及軟硬體時，繳回或刪除舊版本】

十、個資保護認知宣導及教育訓練

1. 定期舉辦全體員工一般訓練，＿＿＿＿至少一次。【註：應有一定頻率，例如每半年或一年】

□個人資料保護相關法令之規定

□所屬人員之責任範圍

□本計畫各項管理程序、機制及措施之要求

2. 定期舉辦個資小組人員（代表人、負責人及管理人員）特殊訓練，＿＿＿＿至少一次。【註：應有一定頻率，例如每半年或一年】

3. 資訊人員定期參加特殊訓練，＿＿＿＿至少一次。【註：應有一定頻率，例如每半年或一年】

4. 留存教育訓練實施紀錄，包括

- 簽到簽退
- 製作會議紀錄
- 課後評量機制

十一、 使用紀錄、軌跡資料及證據保存

（一） 個資之蒐集、處理或利用紀錄

1. 保存方法：＿＿＿＿＿＿【註：依公司實際需求，例如電子資料存於 AWS 雲端】

2. 保存地點：＿＿＿＿＿＿【註：依公司實際需求，例如網站管理系統資料庫】

3. 保存期限：＿＿＿＿＿＿【註：至少 5 年】

（二） 自動化機器設備之軌跡資料

1. 保存方法：_____【註：依公司實際需求，例如電子資料存於地端】

2. 保存地點：_____【註：依公司實際需求，例如本公司機房】

3. 保存期限：_____【註：至少 5 年】

（三） 落實執行個人資料檔案安全維護計畫之證據

1. 保存方法：_____【註：依公司實際需求，例如電子資料存於地端】

2. 保存地點：_____【註：依公司實際需求，例如本公司機房】

3. 保存期限：_____【註：至少 5 年】

十二、 個資安全稽核

1. _____定期檢查或稽核一次【註：通常每一年或兩年】

□自我檢查

□內部稽核

□第三方外部稽核

2. 稽核人員資格

□具個資稽核證照之人員

□管理人員

□法制人員

□資訊安全人員

3. 稽核結果之處理

- 作成評估報告
- 保留稽核紀錄
- 回報管理階層審查
- 立即檢討改善
- 修正本計畫

4. 檢查執行頻率

(1) 本公司為：

□資本額 1000 萬元以下或保有個資 5000 筆以下，定期____【註：通常為半年、1 年或 2 年】執行安全維護措施

□資本額 1000 萬元以上或保有個資 5000 筆以上，每 12 個月定期執行一次安全維護措施

(2) 定期執行安全維護措施內容如下：

- 界定個人資料之範圍
- 個人資料之風險評估
- 檢視個資蒐集目的是否已消失
- 防止外部網路入侵對策
- 演練異常存取行為因應機制
- 檢測系統漏洞及修補
- 更新及執行防毒軟體及檢測惡意程式
- 檢查資通系統使用狀況及存取個資情形
- 檢視個資存取權限
- 全體員工教育訓練
- 代表人及管理人員教育訓練
- 資料安全稽核機制
- 檢視安全維護計畫執行狀況及修正計畫

十三、 委外監督

本公司委託他人蒐集、處理或利用個人資料時，應對委外廠商依個人資料保護法法施行細則第 8 條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。包含：

1. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

2. 委外廠商應採取之措施：

- 配置管理之人員及相當資源。
- 界定個人資料之範圍。

- 個人資料之風險評估及管理機制。
- 事故之預防、通報及應變機制。
- 個人資料蒐集、處理及利用之內部管理程序。
- 資料安全管理及人員管理。
- 認知宣導及教育訓練。
- 設備安全管理。
- 資料安全稽核機制。
- 使用紀錄、軌跡資料及證據保存。
- 個人資料安全維護之整體持續改善。
- 契約中其他指定事項。

3. 有複委託時，本公司之委外廠商應監督受其受託之業者。

4. 委外廠商或其受僱人違反個資法、數位經濟相關產業個人資料檔案安全維護管理辦法、其他個人資料保護法令或其法規命令時，應通知本公司並採取補救措施。

5. 委託關係終止或解除時，委外廠商應返還個人資料儲存載體，並刪除因履行委託契約而持有之個人資料。

6. _____一次定期確認委外廠商個資安全維護措施執行之狀況，並紀錄確認結果。【註：通常每半年或一年】

十四、 業務終止後個人資料處理方法

（一） 人員離職時之資料返還

1. 要求人員返還個人資料之載體，並由專責人員進行檢查。

2. 要求人員刪除因執行業務而持有之個資，並由專責人員進行檢查。

（二） 因業務終止而銷毀證據保存

1. 銷毀：紀錄銷毀之方法、時間、地點及證明銷毀之方式。

2. 移轉：移轉個人資料者，應記錄其原因、對象、方法、時間、地點及受移

轉對象得保有該個人資料之合法依據。

3. 其他刪除、停止處理或利用個人資料：記錄其刪除、停止處理或利用之方法、時間或地點。

4. 上述銷毀、移轉或刪除等紀錄，應保留至少 5 年。

十五、 個人資料安全維護之整體持續改善

（一） 安全維護計畫未落實執行時應採取矯正預防措施

1. 找出缺失之原因，以及評估是否有類似的缺失存在，或之後可能發生缺失的項目。

2. 評估消除缺失項目所須採取的措施，並實際執行。

3. 審查所有已採取的矯正措施的有效性。

4. 將矯正措施更新於本計畫。

5. 將缺失原因、所採取之矯正措施、採取措施的過程、採取措施的結果，以文件化方式保存，做為參考依據及證據。

（二） 定期檢視及修正本計畫

定期檢視頻率：_____定期檢視及修正本計畫一次。修正內容：依據安全維護計畫矯正措施、技術發展、業務調整、法令變化等，更新內容於本計畫。【註：通常每半年或一年】

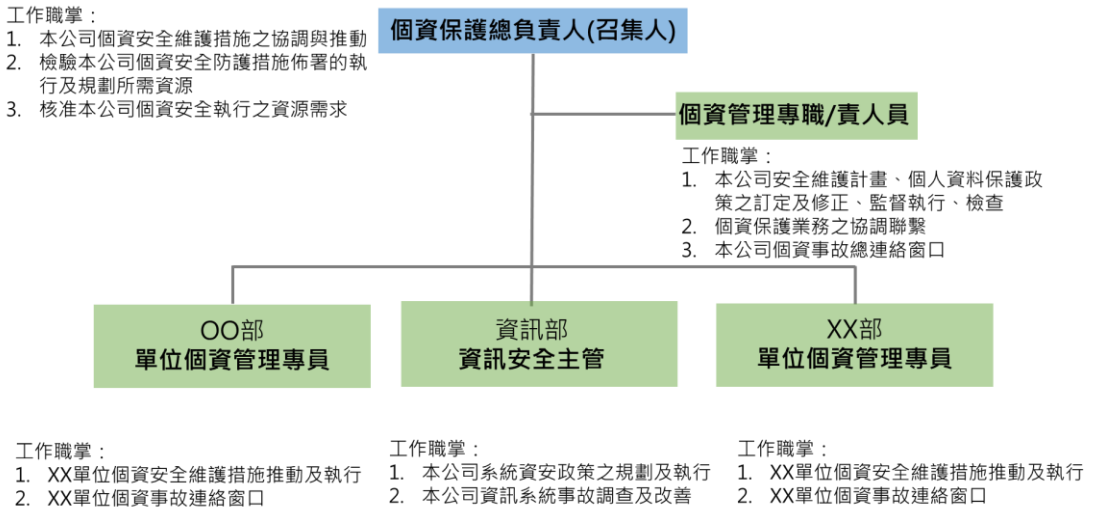
附錄 2：資服業者個資安全維護計畫填寫示範

小叮噹股份有限公司個人資料安全維護計畫

112 年 12 月 15 日 1 版

小叮噹股份有限公司（下稱本公司）依據個人資料保護法、數位經濟相關產業個人資料檔案安全維護管理辦法等相關規範，訂定以下個人資料安全維護計畫（下稱本計畫），作為本公司個人資料保護管理機制之最高指導文件。

一、個資小組



二、個人資料保護管理政策

本公司對內公開周知以下個人資料保護管理政策：

1. 遵守我國個人資料保護相關法令規定。

2. 依照本計畫第六點所列個人資料蒐集、處理及利用之內部管理程序內容，於特定目的範圍內，蒐集、處理或利用個人資料。

3. 依照本計畫第七點所列資料安全管理內容，以可期待之合理安全水準技術保護其所蒐集、處理或利用之個人資料檔案。合理安全水準技術。

4. 本公司之個資聯絡窗口：

(1) 個資當事人行使其個資相關權利或提出相關申訴與諮詢聯絡窗口：_

（個資管理專責人員：技安）

(2) 事故通報個資聯絡窗口：（個資管理專責人員：技安）

5. 緊急應變程序依照本計畫第五點所列之內容進行。

6. 監督委外廠商依照本計畫第十三點所列內容進行。

7. 持續維運安全維護計畫之義務，依照本計畫第十五點所列之內容進行以確保個人資料檔案之安全。

三、清查（盤點）及界定個人資料之範圍

（一） 清查（盤點）及界定頻率：每年 進行清查（盤點）及界定一次。

（二） 蒐集、處理或利用個資之屬性

■所屬人員（含員工、業務、兼職、委外、派遣、顧問、股東等人員）

□消費者

■客戶

■供應商、承包商

（三） 個資種類及目的

檔案名稱	特定目的	個人資料類別(及內容)	預計處理或利用方式
員工資料	○○二 人事管理	識別個人資料(C001) (如姓名、地址、電話、電子郵件等資訊)	進行人事管理措施
		現行之受僱情形(C061) (如工作職稱、工作描述、受僱之條件及期間等資訊)	
		薪資與預扣款(C068) (如薪水、工資、佣金等)	給付薪資
供應商聯絡資料	○六九 契約、類似契約或其他法律關係事務	資料主體之商業活動(C101)(如提供或使用之財貨或服務、商業契約等)	購買商品或服務契約管理，及給付貨款
		辨識財務者(C002) (如金融機構帳戶資訊)	
客戶之消費者資料	一三六 資(通)訊與資料庫管理	識別個人資料(C001) (如姓名、地址、電話、電子郵件等資訊)	受託儲存客戶之消費者資料
		個人描述(C011) (如：年齡、性別等)	

（四） 個資盤點方式

個資檔案名稱	特定目的	個人資料類別及內容	預計處理或利用方式	處理或利用地區	處理或利用期間	資料筆數	建立時間及更新時間	處理及利用軌跡紀錄
001 員工資料	○○二 人事管理	識別個人資料(C001)（如姓名、地址、電話、電子郵件等資訊）	員工資料	台灣地區及本公司關聯方經營業務的其他國家或地區	至使用目的不復存在時	OOO筆	20XX/XX/XX	例：編號520於2023/09/06輸入於OODB2伺服器
	薪資與預扣款(C068)（如薪水、工資、佣金等)	給付薪資						
002 供應商聯絡資料	○六九 契約、類似契約或其他法律關係事務	資料主體之商業活動(C101)(如提供或使用之財貨或服務、商業契約等)	購買商品或服務契約管理	台灣地區	至使用目的不復存在時	OOO筆	20XX/XX/XX	例：編號125於2023/10/02傳輸至XX
003 客戶之消費者資料	一三六 資（通）訊與資料庫管理	識別個人資料(C001)（如姓名、地址、電話、電子郵件等資訊）	受託儲存客戶之消費者資料	台灣地區	10天	OOO筆	20XX/XX/XX	例：編號365於20XX/XX/XX行使刪除權

四、個人資料之風險評估及管理機制

（一） 評估頻率：每年 進行評估一次。

（二） 風險評估表

個資檔案	個資類別 1.一般 2.敏感(財務) 3.特種	個資屬性 1.客戶、供應商及承包商 2.所屬人員 3.消費者	個資檔案價值 (個資類別+個資屬性)	個資筆數 (每月估算)	作業情境及內容	可能風險類型	風險處理對策
例：消費者訂單	2	3	5	1000	外部傳送(串接)	串接渠道有漏洞致外洩	1.尋找漏洞修正協定 2.傳輸資料隱碼
例：廠商聯絡資料	1	1	2	100	保管(地端資料庫)	中釣魚信件致資料庫遭攻擊及外洩	1.加強員工社交工程演練 2.資料庫內資料加密

（三） 風險類型及預訂風險對策

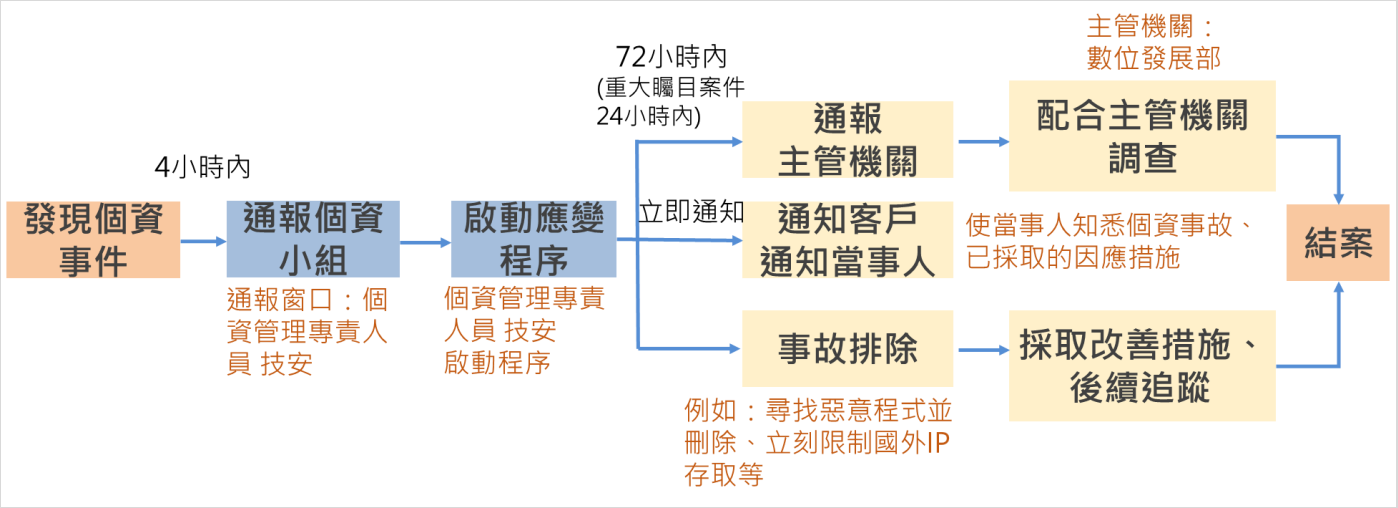
作業情境	作業內容	可能風險類型	風險處理可能對策
加工	輸入/編輯	個資遭竄改	限制輸入/編輯作業人員權限
	輸出/列印	不當存取	權限設定
	掃描	不當存取	權限設定
內部傳輸	人員親送	收發記載不確實以致遺失	確認收受紀錄媒體內容、件數，雙方留存收受紀錄
		USB等外接紀錄媒體遺失	將USB等外接紀錄媒體依儲存個資重要性加以密碼鎖碼或暗號化
	Email	Email傳送中被竊取	將包含個資的文件以附加檔案方式加上設定密碼
	系統/網路	透過網路伺服器傳送時被竊取	個資檔案以VPN或SSL加密傳送
外部傳輸	Email	Email傳送中被竊取	將包含個資的文件以附加檔案方式加上設定密碼
	API串接	串接協定有漏洞	尋找漏洞修正協定、傳輸資料隱碼
保管	個人電腦	安裝非法軟體、上非法線上網站	禁止上非法網站、禁止安裝非法軟體
		不當存取	處理權限設定、防範登錄帳號密碼被他人知悉、不使用密碼記憶功能、定期變更密碼、定期檢查有無不當存取
		個人電腦遭外部攻擊	安裝防毒軟體並定期更新防毒碼、使用弱點掃描
	資料庫/主機伺服器	帳密遭竊致駭客合法登入	使用雙因子認證、鎖定登入IP
		不當存取資料	設定伺服器專用資料夾存取權限，並將存取權限限於該業管人員
		伺服器遭外部攻擊	安裝防毒軟體並定期更新防毒碼、使用弱點掃描
	檔案室/檔案櫃	進入檔案室/櫃取得資料	限制人員進入檔案室、重要資訊應上鎖保管
廢棄	刪除/銷毀	未到期前過失刪除/銷毀	規定各個個資的保存期間，並於確認後才銷燬，取得刪除/銷毀軌跡紀錄由部門主管檢查
		刪除/銷毀處理不夠確實致外洩	規定刪除程序並依程序確實刪除

五、事故之預防、通報及應變機制

（一） 事故應變流程圖

「發生個資事故」後，通報個資小組窗口、並由個資小組啟動應變程序，應變程序至少有 3 項，各項應變程序皆完成後始可結案。

1. 事故通報：72 小時內（重大矚目案件 24 小時內）通報主管機關數位發展部並配合調查。
2. 通知當事人：立即通知客戶並配合協助通知當事人，使當事人知悉個資事故及已採取之因應措施。
3. 事故排除及追蹤：立即採取事故排除措施、改善措施、及後續追蹤。



（二） 事故通報

1. 通報時點：知悉發生事故 72 小時內；若屬重大矚目案件（例如已被全國性媒體報導）24 小時內通報。
2. 通報條件：遇有個人資料安全事故，將危及其正常營運或大量當事人權益。
3. 通報對象：數位發展部。電話：02-23808390；信箱：www-mailbox.adi.gov.tw
4. 通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。（使用數位經濟相關產業個人資料檔案安全維護管理辦法附表二）
   https://law.moda.gov.tw/Download.ashx?FileID=751

附表二　業者個人資料外洩通報表

個人資料侵害事故通報與紀錄表		
業者名稱 通報機關	通報時間:　年　月　日　時　分 通報人:　　簽名(蓋章) 職稱: 電話: Email: 地址:	
事件發生時間		
事件發生種類	☐竊取 ☐洩漏 ☐竄改 ☐毀損 ☐滅失 ☐其他侵害事故	個人資料侵害之總筆數(大約) _____筆 ☐一般個人資料_____筆 ☐特種個人資料_____筆
發生原因及事件摘要		
損害狀況		
個人資料外洩可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於知悉個人資料外洩後72小時通報	☐是　☐否，理由：	

（三） 通知當事人

1. 通知時點：自知悉時起即應盡速通報。
2. 通知條件：遇有個資被竊取、洩漏（個資外洩）或竄改、損毀、滅失之事故。
3. 通知內容：使當事人知悉個資遭外洩或竊取、已採取哪些因應對及修補措施。
4. 通知方式：以簡訊、電子郵件或其他足以使當事人知悉或可得知悉之方式。

六、個人資料蒐集、處理及利用之內部管理程序

（一） 盤點每項個資檔案，確認個資蒐集、處理或利用是否符合法定要件：

1. 特定目的

(1) 利用個資時符合蒐集時之利用目的。

(2) 目的外利用個資，符合個資法第 20 條下列事由：

- 法律明文規定。
- 為增進公共利益所必要，公共利益。
- 為免除當事人之生命、身體、自由或財產上之危險。
- 為防止他人權益之重大危害。
- 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 經當事人同意。(應先告知個資法第 8 條所定應告知事項)
- 有利於當事人權益。
- 特種個資不得目的外利用。

2. 法律依據

(1) 特種個資，符合個資法第 6 條所訂之法律依據

- 法律明文規定。
- 業者履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 當事人自行公開或其他已合法公開之個人資料。
- 學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 經當事人書面同意。(應先告知個資法第 8 條所定應告知事項)【註：但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。】

(2) 一般個資，符合個資法第 19 條之法律依據

- 法律明文規定。
- 與當事人有契約或類似契約之關係，且已採取適當之安全措施。
- 當事人自行公開或其他已合法公開之個人資料。

- 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 經當事人同意。（應先告知個資法第 8 條所定應告知事項）
- 為增進公共利益所必要。
- 個資取自於一般可得之來源。【註：但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。】
- 對當事人權益無侵害。

3. 告知當事人

(1) 告知個資當事人，符合個資法第 8、9 條之規定

A. 直接向當事人蒐集個資時，明確告知當事人下列事項：

- 業者名稱。
- 蒐集之目的。
- 個人資料之類別。
- 個人資料利用之期間、地區、對象及方式。
- 當事人依第三條規定得行使之權利及方式。
- 當事人得自由選擇提供個資時，不提供將對其權益之影響。

B. 蒐集非由當事人提供之個資時，明確告知當事人下列事項：

- 公務機關或非公務機關名稱。
- 蒐集之目的。
- 個人資料之類別。
- 個人資料利用之期間、地區、對象及方式。
- 當事人依第三條規定得行使之權利及方式。

(2) 符合免為告知之情形

A. 直接向當事人蒐集個資時符合免為告知之情形

- 依法律規定得免告知。
- 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
- 告知將妨害公務機關執行法定職務。

- 告知將妨害公共利益。
- 當事人明知應告知之內容。
- 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

B. 蒐集非由當事人提供之個資時符合免為告知之情形

- 依法律規定得免告知。
- 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
- 告知將妨害公務機關執行法定職務。
- 告知將妨害公共利益。
- 當事人明知應告知之內容。
- 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。
- 當事人自行公開或其他已合法公開之個人資料。
- 不能向當事人或其法定代理人為告知。
- 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
- 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

4. 最小化原則（比例原則）

蒐集個資時不蒐集與利用目的無關的個資。

5. 國際／境外傳輸之限制、告知

本公司將個人資料作國際傳輸時，將檢視是否受數位發展部依個人資料保護法第 21 條所為之限制，並且告知當事人其個人資料所將國際傳輸之區域。本公司將對資料接收方為下列事項之監督：一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。二、當事人行使個人資料保護法第 3 條所定權利之相關事項。

（二） 受理當事人請求權利之程序

1. 受理內容

(1) 拒絕行銷之處理程序

(2) 受理當事人行使個資法第 3 條權利之程序

(3) 受理個資更正之程序

2. 拒絕行銷受理方式：

(1) 當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

(2) 首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

(3) 提供當事人免費、快速、容易表達之簡便方式。

3. 當事人行使個資法第 3 條權利受理方式：

(1) 告知當事人得依個資法第 3 條規定得行使之權利及方式

(2) 至少與蒐集當事人個資相同之方式、管道、難易度相同。

(3) 受理後處理方式包含：

- 確認當事人或其代理人之身分。
- 檢視是否符合個資法第 10 條但書、第 11 條第 2 項但書及第 11 條第 3 項但書所定得拒絕其請求之事由。
- 拒絕當事人行使權利者，附理由通知當事人。
- 當事人請求為准駁決定及延長決定期間之程序，並應確保符合個資法第 13 條之規定。
- 當事人請求更正或補充其個人資料者，其應釋明之事項。
- 當事人查詢、請求閱覽或製給複製本之請求酌收必要成本費用者，應明定其收費標準。

4. 個資更正受理方式：

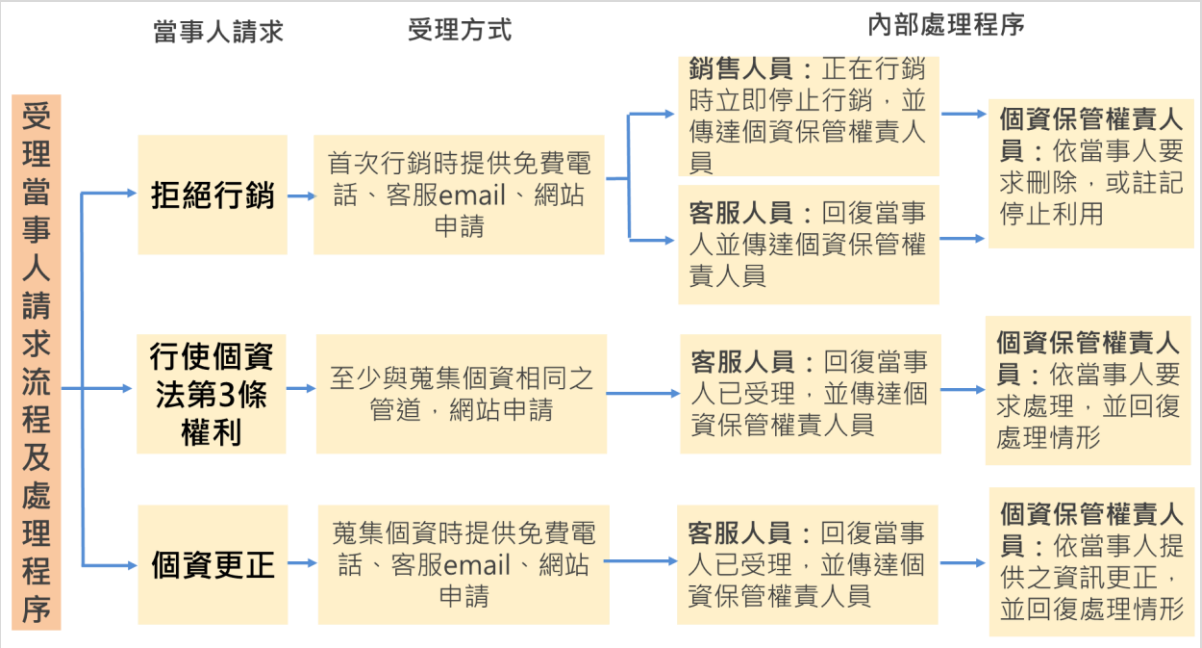
(1) 維護個人資料之正確，並主動或依當事人之請求更正或補充之。

(2) 提供當事人免費、快速、容易表達之簡便方式請求更正或補充之。

(3) 個資正確性有爭議者，應主動或依當事人之請求停止處理或利用。【註：因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。】

(4) 因可歸責於本公司之事由，未為更正或補充之個資，應於更正或補充後，通知曾提供利用之對象。

5. 受理流程圖：



七、資料安全管理

本公司之 線上購物網站管理 系統、公司 OA 區電腦、共用區 設備，採取以下資料安全管理措施：

1. 加密：儲存於 管理系統資料庫 之資料採取 AES256 等加密措施。

2. 備份：備份資料採取 加密儲存、自動備份、自動壓縮、自動金鑰加密等 之保護措施。

3. 傳輸安全：管理系統資料庫 之資料透過 API 傳輸時，採取適當 SSL 傳輸加密機制、資料顯示之隱碼機制 之安全措施。

4. 外部網路入侵對策：

■建置防火牆：管理系統伺服器及 OA 區網路防火牆只開放必要的通訊埠對外連線 ，並 3 個月 定期更新一次。

■建置應用程式防火牆：網站安裝應用程式防火牆監測、過濾、阻斷可疑的流量，並 3 個月 定期更新一次。

■電子郵件過濾機制：員工電子郵件系統採取 OO 過濾系統，並 3 個月 定期更新一次。

■端點防護：OA 區電腦、共用區設備採取端點防護，並每年 定期更新一次。

□其他入侵偵測設備：_____，並_____(時間)一次定期更新一次。

5. 異常存取資料行為之監控及因應演練：設定異常存取資料行為監控機制；並 每年 定期演練異常存取資料行為因應機制。【註：通常每半年或一年】

6. 檢測系統漏洞及修補： 每年 定期一次透過 網站弱點掃描、主機弱點掃描 檢測系統漏洞，並修補漏洞至無中風險及高風險漏洞。

7. 防毒軟體及惡意程式檢測：

(1) 設備及系統隨時更新及執行防毒軟體。

(2) 每年 定期執行惡意程式檢測一次。

8. 密碼及認證機制：

■密碼【註：帳號及密碼須符合一定之複雜度】

■其他認證機制：雙因子認證：密碼、簡訊認證碼

9. 避免利用真實個資測試：

(1) 處理個資之資通系統進行測試時避免使用真實個資。

(2) 使用真實個資者，應訂定使用規範。

10. 資訊系統變更：處理個資之資通系統有變更時，應確保其安全性未降低。

11. 定期檢查： 每年 一次定期檢視處理個資之資通系統，檢查其使用狀況及存取個資之情形。

12. 個資隱碼：針對本公司 網站管理系統資料庫個資透過 API 傳輸 之個資使用情境，採行個資之隱碼機制。隱碼機制： SSL 傳輸加密機制、資料顯示之隱碼機制

13. 其他資料安全措施：_____

八、人員安全管理

1. 保密義務約定：與所屬人員約定保密義務，約定方式：簽署保密協議書

2. 識別人員：識別業務內容涉及個資蒐集、處理或利用之人員。識別方式：依專案內容或業務屬性判斷會蒐用個資的人員

3. 人員存取權限之控制：依業務特性、內容及需求，設定所屬人員接觸個資之權限，並定期檢視適當性及必要性。

■實體空間人員進出管制措施：辦公室門禁、檔案室門禁、機房門禁

■系統共用文件區存取管制措施：共用區個別檔案僅該涉及專案之人員才有存取權限

□其他：_____

4. 人員離職時之資料返還程序：要求離職人員返還個人資料之載體，並由專責人員進行檢查；要求離職人員刪除因執行業務而持有之個資，並由專責人員進行檢查

九、設備安全管理

1. 儲存媒介物：依存有個資之儲存媒介物（紙本、光碟片、電腦、自動化機器設備及其他媒介物等）之特性及使用方式，訂定以下管理規範：

■採取設備維護安全管理措施：端點防護

■採取儲放環境安全管理措施：檔案室環境規則、共用區存取規則

□其他：_____

2. 人員保管規範：針對所屬人員保管個人資料之儲存媒介物，訂定管理規範：該設備存有之資料涉及機密，不得接取可連接外部網路之主機

3. 人員進出管制規範：針對存放儲存媒介物之環境，採取進出管制規範：檔案室門禁管制

4. 過期資料及設備處理措施：對於過期資料及軟硬體的處理方式應採取以下措施：提供新版本之資料及軟硬體時，繳回或刪除舊版本

十、個資保護認知宣導及教育訓練

1. 定期舉辦全體員工一般訓練，每年至少一次。

■個人資料保護相關法令之規定

■所屬人員之責任範圍

■本計畫各項管理程序、機制及措施之要求

2. 定期舉辦個資小組人員（　代表人、負責人及管理人員）特殊訓練，每年至少一次。

3. 資訊人員定期參加特殊訓練，每年至少一次。

4. 實施之佐證紀錄

- 簽到簽退
- 製作會議紀錄
- 課後評量機制

十一、　使用紀錄、軌跡資料及證據保存

（一） 個資之蒐集、處理或利用紀錄

1. 保存方法：電子資料存於 AWS 雲端

2. 保存地點：線上購物網站管理系統資料庫

3. 保存期限：5 年

（二） 自動化機器設備之軌跡資料

1. 保存方法：電子資料存於本公司自行管理之伺服器

2. 保存地點：本公司機房

3. 保存期限：5 年

（三） 落實執行個人資料檔案安全維護計畫之證據

1. 保存方法：電子資料存於本公司自行管理之伺服器

2. 保存地點：本公司機房

3. 保存期限：5 年

十二、 資料安全稽核

1. 每年 定期檢查或稽核一次

■自我檢查

■內部稽核

□第三方外部稽核

2. 稽核人員資格

■具個資稽核證照之人員

□管理人員

■法制人員

■資訊安全人員

3. 稽核結果之處理

- 作成評估報告
- 保留稽核紀錄
- 回報管理階層審查
- 立即檢討改善
- 修正本計畫

4. 檢查執行頻率

(1) 本公司為：

□資本額 1000 萬元以下或保有個資 5000 筆以下者，定期___執行安全維護措施

■資本額 1000 萬元以上或保有個資 5000 筆以上者，每 12 個月定期執行一次安全維護措施

(2) 定期執行安全維護措施內容如下：

- 界定個人資料之範圍
- 個人資料之風險評估

- 檢視個資蒐集目的是否已消失
- 防止外部網路入侵對策
- 演練異常存取行為因應機制
- 檢測系統漏洞及修補
- 更新及執行防毒軟體及檢測惡意程式
- 檢查資通系統使用狀況及存取個資情形
- 檢視個資存取權限
- 全體員工教育訓練
- 代表人及管理人員教育訓練
- 資料安全稽核機制

十三、 委外監督

本公司委託他人蒐集、處理或利用個人資料時，應對委外廠商依個人資料保護法法施行細則第 8 條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。包含：

1. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

2. 委外廠商採取措施：

- 配置管理之人員及相當資源。
- 界定個人資料之範圍。
- 個人資料之風險評估及管理機制。
- 事故之預防、通報及應變機制。
- 個人資料蒐集、處理及利用之內部管理程序。
- 資料安全管理及人員管理。
- 認知宣導及教育訓練。
- 設備安全管理。
- 資料安全稽核機制。
- 使用紀錄、軌跡資料及證據保存。
- 個人資料安全維護之整體持續改善。
- 契約中其他指定事項。

3. 有複委託時，本公司之委外廠商應監督受其受託之業者。

4. 委外廠商或其受僱人違反個資法、數位經濟相關產業個人資料檔案安全維護管理辦法、其他個人資料保護法律或其法規命令時，應向本公司通知之事項及採行之補救措施。

5. 委託關係終止或解除時，個人資料載體之返還，及委外廠商履行委託契約以儲存方式而持有之個人資料之刪除。

6. 每年 一次定期確認委外廠商執行之狀況，並紀錄確認結果。

十四、 業務終止後個人資料處理方法

（一） 人員離職時之資料返還

1. 要求離職人員返還個人資料之載體，並由專責人員進行檢查。

2. 要求離職人員刪除因執行業務而持有之個資，並由專責人員進行檢查。

（二） 因業務終止而銷毀證據保存

1. 銷毀：紀錄銷毀之方法、時間、地點及證明銷毀之方式。

2. 移轉：移轉個人資料者，應記錄其原因、對象、方法、時間、地點及受移轉對象得保有該個人資料之合法依據。

3. 其他刪除、停止處理或利用個人資料：記錄其刪除、停止處理或利用之方法、時間或地點。

4. 上述銷毀、移轉或刪除等紀錄，應保留至少 5 年。

十五、 個人資料安全維護之整體持續改善

（一） 安全維護計畫未落實執行時應採取矯正預防措施

1. 找出缺失之原因，以及評估是否有類似的缺失存在，或之後可能發生缺失的項目。

2. 評估消除缺失項目所須採取的措施，並實際執行。

3. 審查所有已採取的矯正措施的有效性。

4. 將矯正措施更新於本計畫。

5. 將缺失原因、所採取之矯正措施、採取措施的過程、採取措施的結果，以文件化方式保存，做為參考依據及證據。

（二） 定期檢視及修正本計畫

定期檢視頻率：每年定期檢視及修正本計畫一次。修正內容：依據安全維護計畫矯正措施、技術發展、業務調整、法令變化等，更新內容於本計畫。【註：通常每半年或一年】

附錄 3：業者個人資料蒐集、處理及利用之委外業務監督管理自評表範例

業者委託資服業者進行個人資料蒐集、處理及利用之業務時，應依「個人資料保護法施行細則」第 8 條、「數位經濟相關產業個人資料檔案安全維護管理辦法」第 19 條第 1 項負監督委外廠商義務。

數位發展部數位產業署提供以下範本，使業者監督委外廠商時，提供給受委託之資服業者自評時參考。

受託廠商名稱：＿＿＿＿＿＿＿＿＿＿＿＿（委外廠商資服業者填寫）

自評人員：＿＿＿＿＿＿

自評日期：＿＿年＿＿月＿＿日

項次	自評內容	自評結果	說明
個資保護政策與安全維護計畫			
1	是否訂定個人資料保護管理政策，並對內公開周知？	□符合 □不符合 □不適用	
2	是否訂定個人資料檔案安全維護計畫或適當安全維護措施或建置通過第三方驗證之資訊安全管理系統並公布施行？	□符合 □不符合 □不適用	
個人資料生命週期行為規範			
3	對於個人資料之蒐集、處理或利用之範圍、類別、特定目的與期間是否明確律定？	□符合 □不符合 □不適用	
4	對於個人資料之蒐集、處理、利用、傳輸或刪除，是否訂定管理作業程序並公布施行？	□符合 □不符合 □不適用	
個人資料盤點與風險管理			
5	對所保有之個人資料，是否定期實施	□符合	

	個人資料盤點作業？	□不符合 □不適用	
6	是否適時維護或更新個人資料檔案清冊？	□符合 □不符合 □不適用	
7	是否定期實施個人資料風險評鑑作業？	□符合 □不符合 □不適用	
8	對於個人資料風險評鑑結果，是否考量業務性質、個人資料存取環境、個人資料傳輸之工具與方法及個人資料之種類、數量等因素，採取適當之人員、作業、設備及技術之安全管理措施？	□符合 □不符合 □不適用	
人員管理			
9	是否訂定人員管理作業程序並公布施行？	□符合 □不符合 □不適用	
10	是否定期對內部人員實施資安認知宣導及教育訓練？	□符合 □不符合 □不適用	
11	執行個人資料蒐集、處理及利用之人員，是否取得資通安全專業證照？	□符合 □不符合 □不適用	
日常維運作業			
12	是否定期識別、審視防火牆、主機系統、資料庫等重要設備之異常告警機制並留存至少 5 年之 LOG？	□符合 □不符合 □不適用	
13	系統異動或登入是否取得授權？	□符合	

		□不符合 □不適用	
14	是否進行系統運作與維護之需求評估，並依此建立適當的系統安全檢測機制？	□符合 □不符合 □不適用	
15	是否依據各項變更之需求進行變更作業程序，並留存相關紀錄?	□符合 □不符合 □不適用	
16	是否依據系統各項目標與需求，研擬適當的防護措施檢核表?	□符合 □不符合 □不適用	
17	是否要求委外廠商定期提出系統安全之風險評估報告?	□符合 □不符合 □不適用	
內部稽核			
18	是否定期實施資訊安全或個人資料保護之內部稽核並提出稽核報告？	□符合 □不符合 □不適用	
19	稽核結果若有不符合法令或有違法之虞或缺失者，是否規劃採取包含修正個人資料保護管理政策及個人資料檔案安全維護計畫之改善及預防措施？	□符合 □不符合 □不適用	
資安事故通報與應變			
20	是否訂定資安事故之通報及應變程序，包含知悉資安/個資事故發生或有發生之虞之相關通報時效規定、通報方式、事故調查、處理及改善流程並公布施行？	□符合 □不符合 □不適用	
21	是否訂定違反個人資料保護法、其他	□符合	

	個人資料保護法律或其法規命令時之通知之事項及採行之補救措施作業程序並公布施行？	□不符合 □不適用	
受託業務之複委託選任與監督			
22	受託業務之複委託事項，是否經委託機關之書面同意後實施？	□符合 □不符合 □不適用	
23	是否訂定委託之標準及評估機制並公布施行？	□符合 □不符合 □不適用	
24	是否於委託契約或相關文件中明確約定適當之個人資料保護有關事項之監督方式，並留存監督之紀錄？	□符合 □不符合 □不適用	
委託關係終止或解除			
25	是否訂定委託關係終止或解除時，個人資料載體之返還，及履行委託契約以儲存方式而持有之個人資料之刪除作業程序並公布施行？	□符合 □不符合 □不適用	
文件化			
26	是否對於個人資料之蒐集、處理、利用、國際傳輸或刪除均留存使用紀錄或軌跡資料？	□符合 □不符合 □不適用	

附錄 4：資服業者落實個人資料安全維護計畫自我檢查表範例

資服業者落實個人資料安全維護計畫自我檢查表			
業者名稱：		檢查時間：	檢查人：
編號	檢查項目	適用情形	檢查情形說明
1. 配置管理之人員及相當資源			
1.1 配置個資保護總負責人			
1.1.1	由高階管理者擔任個資安全總負責人 可由總經理、代表人擔任、副總經理級或資安長級擔任	□適用 □不適用 說明：	□由_____(職位)擔任個資安全總負責人 □業者之代表人或其授權人員核定業者安全維護計畫、個資保護政策 □確保有關個資安全角色與職權之分配與傳達 □統籌各部門、協調與推動個資安全相關事宜及所需之資源 □檢驗所有資訊保護的防護措施的正確完成執行 □其他：
1.2 建立個資小組及配置個資管理專員			
1.2.1	建立個資小組	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 5 條 □不適用 說明：	□建立個資小組 □訂定及修正安全維護計畫、個資保護政策 □由高階管理者擔任個資小組總召集人 □配置聯絡窗口、安全維護計畫檢核人員、資訊人員、執行人員等 □其他：
1.2.2	配置管理人員（一位或以上）	□適用 □不適用 說明：	□有配置管理人員辦理個資安全維護事項之落實 □（建議）業者之總管理人員為專責/職人員 □各部門配置管理人員 □其他：
2.界定及盤點個人資料之範圍			

2.1 蒐集處理利用個人資料之告知			
2.1.1	「蒐集處理利用個人資料」告知義務 除有免告知事由，應對資料當事人踐行告知「當事人得行使權利」之義務	□適用 個人資料保護法第 8 條	□蒐集、處理、利用個人資料時有皆盡告知義務
2.2 界定個人資料之範圍			
2.2.1	蒐集、處理、利用個資之對象	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 6 條 □不適用 說明：	□員工 □客戶承辦人 □上下游供應商承辦人 □受委託處理個資 □維修時接觸個資 □其他：
2.2.2	界定個人資料範圍 建議使用法務部訂定之「個人資料保護法之特定目的及個人資料之類別」敘明所蒐集個資之特定目的及類別	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 6 條 □不適用 說明：	□定期界定頻率：_____ □敘明界定之特定目的及個資類別 □使用法務部訂定之「個人資料保護法之特定目的及個人資料之類別」敘明目的類別 □其他：
2.3 個人資料盤點（清查）			
2.3.1	清查確認所蒐集、處理或利用之個人資料現況 建議可使用「分析個資流程」方式	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 6 條 □不適用 說明：	□定期清查頻率：_____ □清查各作業流程表單及紀錄，辨識、歸納、整理成個人資料檔案 □使用個人資料盤點表檢視個資檔案，確認檔案名稱、保有依據、特定目的、個資種類 □使用個人資料盤點表檢視個資檔案之生命週期過程內容及是否合法 □其他方式：
3.風險評估與管理機制			
3.1 風險評估			
3.1.1	營運風險評估	□適用 □不適用	□識別委託者業別 □識別應遵循法令及評估法遵

		說明：	成本風險 □識別應遵守契約條款及評估遵守契約成本風險 □其他：
3.1.2	系統或設備之風險評估	□適用 □不適用 說明：	□評估業者內部電腦及資訊系統 □評估儲存客戶之消費者個資之系統或設備 □其他：
3.1.3	蒐集、處理、利用作業之風險評估 蒐集、處理與利用可能產生的各種作業情境及內容	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 7 條 □不適用 說明：	□定期評估頻率：_____ □加工（例如輸入、編輯、輸出、掃描等） □內部傳輸（例如 E-mail、網路伺服器） □外部傳輸（例如 E-mail、網路伺服器） □保管儲存（載體包含個人電腦、資料庫、主機伺服器）（不當存取、個人電腦遭外部攻擊） □廢棄（例如刪除、資料銷毀不夠落實致外洩） □其他：
3.2 風險管理			
3.2.1	風險管理 針對風險評估結果提出預定或已採取之具體風險管理措施或風險處理對策	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 8 條 □不適用 說明：	□加工管理方式： □內部傳輸管理方式： □外部傳輸管理方式： □保管儲存管理方式： □廢棄管理方式： □其他：
4.事故之預防、通報及應變機制			
4.1 事故應變			
4.1.1	事故發生時應變 列舉發生時、發生後之可能做法或執行流程，包含降低、控制當事人損害之方式	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 8 條	□建立做法或執行流程 □立即通報主管機關 □立即通知客戶 □協助客戶通知其消費者 □調查事件成因

		□不適用 說明：	□立即採取補救措施（尋找惡意程式等） □重新評估與客戶間資安責任 □至少一年一次事故演練並檢討 □其他：
4.2 事故通報			
4.2.1	通報主管機關 敘明以下內容 通報時點：知悉發生事故 72 小時內 通報條件：資服業者遇有消費者個人資料安全事故，將危及其正常營運或大量當事人權益者。 通報對象：資服業者應通報數位發展部，或通報地方政府時副知數位發展部。 通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。 延遲通報：無法於時限內通報或無法於當次提供通報內容中的全部資訊時，應附延遲理由或分階段提供。	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 8 條	□通報時點： □通報條件： □通報對象： □通報內容： □延遲通報： □其他：
4.2.2	資服業者通知客戶及其消費者 敘明以下內容 通知時點：盡速。 通知事由：資服業者遇有客戶之消費者個資被竊取、洩漏(個資外洩)或竄改、損毀、滅失之事故。 通知內容：使客戶知悉個資遭竊取、已採取的因應措施、通知當事人的時間和方法。 通知方式：以簡訊、電子郵件等	□適用 □不適用 說明：	□通知客戶 □協助通知消費者 □通知時點： □通知條件： □通知內容： □其他：

	其他足以使當事人知悉或可得知悉之方式。		
4.2.3	業者通知消費者 敘明以下內容 通知時點：盡速。 通知事由：業者遇有消費者個資被竊取、洩漏(個資外洩)或竄改、損毀、滅失之事故。 通知內容：使消費者知悉個資遭竊取、已採取的因應措施、通知當事人的時間和方法。 通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。	□適用 □不適用 說明：	□通知消費者 □通知時點： □通知條件： □通知內容： □其他：
4.3 事故修補改善及預防措施			
4.3.1	事故發生後矯正 研議矯正改善措施之機制	□適用 □不適用 說明：	□建立做法或執行流程 □改善資安措施（必須採取） □改變個資蒐集處理利用方式（選擇採取） □重新評估與客戶間資安責任 □其他：
5.內部管理程序			
5.1 個人資料之蒐集、處理或利用程序			
5.1.1	特種個資	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 9 條第 1 款 □不適用 說明	□蒐集、處理或利用特種個資 □檢視是否符合個資法第 6 條第 1 項但書所定情形 □其他：
5.1.2	一般個資蒐集或處理	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 9 條第 2、4 款 □不適用 說明	每筆個資檔案皆有紀錄： □以何種方式蒐集之個人資料 □如何向當事人告知蒐集之目的，或變更使用之目的 □蒐集符合個資法第 19 條第 1 項之何項法定依據 □以符合法規要求方式取得當

			事人同意 □以最小化原則蒐集 □以何種方式處理 □其他：
5.1.3	一般個資利用	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 9 條第 3 款 □不適用 說明	□敘明以何種方式利用及行銷 □敘明拒絕行銷時的後續處理機制為何 □其他：
5.2 受理當事人行使權利之程序			
5.2.1	受理程序 於個人資料安全維護計畫中敘明受理當事人行使權利之程序	□適用 □不適用 說明：	□建立受理當事人行使權利之程序 □使當事人知悉受理程序流程 □以文字使當事人知悉 □以流程圖使當事人知悉
5.2.2	拒絕行銷 利用個資行銷而當事人表示拒絕接受行銷者，確保符合個資法第 20 條第 2、3 項規定	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 9 條第 5 款 □不適用 說明：	□當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷 □首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用 □提供當事人免費、快速、容易表達之簡便方式
5.2.3	當事人行使個資法第 3 條權利 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。 除有免告知事由，應對資料當事人踐行告知「當事人得行使權利」之義務	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 9 條第 6 款 □不適用 說明	□告知當事人得依個資法第 3 條規定得行使之權利及方式 □至少與蒐集當事人個資相同之方式、管道、難易度相同。 □受理後處理方式是否包含： □確認當事人或其代理人之身分 □檢視是否符合個資法第 10 條但書、第 11 條第 2 項但書及第 11 條第 3 項但書得拒絕其請求之事由 □拒絕當事人行使權利者，應附理由通知當事人 □就當事人請求為准駁決定及延長

			決定期間之程序，並應確保符合本法第 13 條之規定 □當事人請求更正或補充其個人資料者，其應釋明之事項 □就當事人查詢、請求閱覽或製給複製本之請求酌收必要成本費用者，應明定其收費標準
5.2.4	個資更正 維護個資正確性之機制	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 9 條第 7 款 □不適用 說明	□維護個人資料之正確，並主動或依當事人之請求更正或補充之。 □提供當事人免費、快速、容易表達之簡便方式請求更正或補充之。 □個資正確性有爭議時，以個資法第十一條第一項、第二項及第五項規定處理。
5.3 國際／境外傳輸			
5.3.1	是否有國際／境外傳輸 業者之伺服器或資料庫位在我國以外之國家地區，則有個人資料為國際／境外傳輸之情形	□適用 □不適用 說明：	□有國際／境外傳輸 □傳輸地區： □傳輸方式： □無國際／境外傳輸
5.3.2	檢視是否受主管機關數位發展部限制	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 10 條 □不適用 說明：	□有檢視限制 □未檢視限制 □限制內容：
5.3.3	告知「個資有國際／境外傳輸」義務	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 10 條 □不適用 說明：	□告知客戶，其消費者之個人資料會傳輸至我國以外區域處理、利用 □告知個資當事人，其個人資料會傳輸至我國以外區域處理、利用
5.4 委託他人蒐集、處理或利用個人資料之管理程序			
5.4.1	委託他人蒐集、處理或利	□適用	□無委託他人蒐集個人資料之

	用個人資料之管理程序	個人資料保護法施行細則第 8 條 □不適用 說明：	情形 □有委託他人蒐集、處理或利用個人資料，受託者進行個資安全維護之監督管理 □預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間 □於契約中敘明個資安全維護責任之事項 □對受託者 1 年檢查____次受託者採取措施 □受託者複委託時有監督複受託者 □受託者或其受僱人違反個資相關法規時，向本公司通知事項及採行補救措施 □本公司對受託者有保留指示者，其保留指示之事項 □委託關係終止或解除時，個資載體之返還，及受託者履行委託契約以儲存方式而持有之個資料刪除
5.5 業務終止後有關於個人資料之處理方式			
5.5.1	特定業務減少或終止	□適用 □不適用 說明：	□建立業務項目終止時個資處理方式 □個資刪除或移轉之程序及佐證 □個資移轉之原因、對象、方法、時間、地點、受移轉對象得保有該個人資料之合法依據 □使資料當事人知悉其個資被移轉至他業者 □使當事人能行使個資法第 3 條之權利
5.5.2	法人格消滅	□適用 □不適用 說明：	□建立法人格消滅時個資處理方式 □個資刪除或移轉之程序及佐證 □個資移轉之原因、對象、方法、時間、地點、受移轉對象得保有該個人資料之合法依據。 □使資料當事人知悉其個資被移轉

			至他業者 □使當事人能行使個資法第 3 條之權利
5.5.3	個資移轉予其他法人	□適用 □不適用 說明：	□建立移轉個資處理方式 □個資刪除或移轉之程序及佐證 □個資移轉之原因、對象、方法、時間、地點、受移轉對象得保有該個人資料之合法依據。 □使資料當事人知悉其個資被移轉至他業者 □使當事人能行使個資法第 3 條之權利
5.6 **定期檢視特定目的是否已消失或期限已屆滿**			
5.6.1	特定目的已消失或期限已屆滿	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 9 條第 8 款 □不適用 說明	□定期檢視頻率：_____ □敘明以何種方式檢視特定目的已消失或期限已屆滿：_____ □敘明已消失或已屆滿後主動刪除 □其他：
6. 資料安全管理及人員管理			
6.1 資料安全管理措施			
6.1.1	基本資料安全管理措施	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 11 條第 1 項 □不適用 說明：	□資料加密機制：_____ □對備份資料採取適當保護措施 □傳輸資料時採取適當保護措施：_____ □其他：
6.1.2	以資通系統處理個資	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 11 條第 2 項 □不適用 說明：	□外部網路入侵對策 □定期執行頻率：_____ □防火牆：_____ □防火牆更新頻率：_____ □電子郵件過濾機制更新頻率：__ □端點防護更新頻率：_____ □入侵偵測設備：_____ □異常存取資料行為之監控

			及因應演練 □定期執行頻率：_____ □檢測系統漏洞及修補 □定期執行頻率：_____ □檢測工具：_____ □檢測時間及頻率：_____ □修補情形：_____ □防毒軟體及惡意程式檢測 □防毒軟體隨時更新及執行 □惡意程式檢測執行頻率：_____ □密碼及認證機制 □密碼符合一定複雜度：_____ □其他認證機制 □避免利用真實個資測試 □資訊系統變更時確保其安全性未降低 □定期檢查資通系統使用情況及個資存取情形 □定期執行頻率：_____ □個資（傳輸時）隱碼 □傳輸時 □提供電子商務時 □其他使用情境：_____ □其他：
6.2 人員安全管理措施			
6.2.1	基本人員安全管理措施	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第12條 □不適用 說明：	□人員保密義務約定 □識別業務內容涉及個資蒐集、處理或利用之人員 □人員存取權限之控制 □人員離退時之資料返還 □其他：
6.2.2	分散式管理或沒有固定辦公場所之人員安全管理措施	□適用 □不適用 說明：	□人員存取紀錄 □資料返還紀錄 □其他：
7. 認知宣導及教育訓練			
7.1 內部員工教育訓練			

7.1.1	內部員工教育訓練 訓練內容：個人資料保護相關法令之規定；所屬人員之責任範圍；本計畫各項管理程序、機制及措施之要求 頻率：敘明實施頻率，規模較小業者至少於業者資安或個資政策更新時實施。 程序；訂定實施頻率；每次宣導或訓練時訂定主題、議程，且實施簽到、製作會議紀錄、課後評量機制	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第13條 □不適用 說明：	□訓練內容： □訓練頻率：_____至少1次 □訓練紀錄： □其他：
7.1.2	個資小組人員（代表人、負責人及管理人員）特殊教育訓練	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第13條 □不適用 說明：	□訓練內容：於安全維護計畫所擔負之任務及角色 □訓練頻率：_____至少1次 □訓練紀錄： □其他：
7.2 外部客戶認知宣導			
7.2.1	外部客戶認知宣導	□適用 □不適用 說明：	□契約簽訂前向該客戶揭露其個人資料安全維護措施 □使客戶認知使用系統時所需安全環境 □其他認知宣導措施：
8.設備安全管理措施			
8.1	基本設備安全管理措施	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第14條 □不適用 說明：	□設備維護安全管理措施 □儲放環境安全管理措施 □人員保管規範 □人員進出管制規範 □過期資料及軟硬體的處理方式 □其他：
9.使用紀錄、軌跡資料及證據保存			
9.1	使用紀錄及軌跡資料證據保存 至少五年：a.個人資料使用紀	□適用 數位經濟相關產業個人資料檔案安全	□個資之蒐集、處理或利用紀錄 □保存方法：_____ □保存地點：_____

	錄；b.自動化機器設備之軌跡資料；c.落實執行個人資料檔案安全維護計畫之證據	維護管理辦法第16條第1項 □不適用 說明：	□保存____年 □自動化機器設備之軌跡資料 □保存方法：_____ □保存地點：_____ □保存____年 □落實執行個人資料檔案安全維護計畫之證據 □保存方法：_____ □保存地點：_____ □保存____年 □其他：
9.2	因業務終止而銷毀證據保存	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第16條第2項 □不適用 說明：	□有紀錄銷毀方法、時間、地點及證明銷毀之方式 □有紀錄移轉原因、對象、方法、時間、地點及受移轉對象得蒐集該個人資料之合法依據 □其他：
10.資料安全稽核機制			
10.1	自我檢查個資安全維護	□適用 □不適用 說明：	□1年至少____次自我檢查個資安全維護執行狀況 □提出評估報告 □採行改善機制 □其他：
10.2	內部個資安全維護稽核機制	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第15條 □不適用 說明：	□1年至少____次內部稽核個資安全維護執行狀況 □內稽人員資格 □合格稽核資格 □管理人員 □法制人員 □資訊安全人員 □稽核結果之處理 □作成評估報告 □保留稽核紀錄 □回報管理階層審查 □立即檢討改善 □修正個資安全維護計畫

			□其他：
10.3	外部個資安全維護稽核機制	□適用 □不適用 說明：	□委請第三方稽核 □委請第三方驗證機構稽核 □其他：
10.4	執行頻率檢查	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第18條 □不適用 說明：	□資本額1000萬元以下或保有個資5000筆以下者，定期_____執行一次安全維護措施 □資本額1000萬元以上或保有個資5000筆以上者，有定期每12個月執行一次安全維護措施 □界定個人資料之範圍 □個人資料之風險評估 □檢視個資蒐集目的是否已消失 □防止外部網路入侵對策 □演練異常存取行為因應機制 □檢測系統漏洞及修補 □更新及執行防毒軟體及檢測惡意程式 □檢查資通系統使用狀況及存取個資情形 □檢視個資存取權限 □全體員工教育訓練 □代表人及管理人員教育訓練 □資料安全稽核機制 □檢視安全維護計畫執行狀況及修正計畫 □其他：
11.持續改善措施			
11.1	持續改善措施	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第17條 □不適用 說明：	□敘明安全維護計畫未落實執行時應採取矯正預防措施 □敘明定期檢視或修正本計畫 □其他：

附錄 5：資服業者資訊安全管理措施自我檢查表範例

資服業者資訊安全管理措施自我檢查表			
公司名稱：		檢查時間：	檢查人：
編號	檢查項目	適用情形	檢查情形說明
1.營運管理面			
1.1 資訊安全權責			
1.1.1	由高階管理者擔任資訊安全總負責人	□適用 □不適用 說明：	□由_____(職位)擔任
1.1.2	資訊安全總負責人應確保有關資安角色與職權之分配與傳達	□適用 □不適用 說明：	□制定公司內部權責
1.1.3	資訊安全總負責人應對資安充分支持及承諾	□適用 □不適用 說明：	□支持及承諾事項：
1.1.4	資訊安全總負責人應對服務提供之資安給予充分支持	□適用 □不適用 說明：	□支持及承諾事項：
1.1.5	高階管理者宜提供資安訓練之資源	□適用 □不適用 說明：	□提供資安訓練之資源
1.2 內部營運之資訊安全管理制度			
1.2.1	內部營運之資訊安全管理制度	□適用 □不適用 說明：	□考量並敘明營運時所面對的內外部議題 □制定政策，內容包含： - 資訊安全的目標 - 概要資訊安全原則的需求 □其他：
2.技術防護面			
2.1 資訊安全作業與保護			
2.1.1	資訊系統與設備盤點	□適用 □不適用 說明：	□內部電腦系統 □內部資訊系統 □儲存客戶之消費者個人資料之系統及設備 □其他：

2.1.2	確立系統作業流程的控管方式 系統作業流程可包含涉及變更時之變更控制方法、容量管理、開發測試與運作環境的分隔等	□適用 □不適用 說明：	□防範惡意程式 □備份 □存錄與監控 □確保作業系統完整性 □防範技術脆弱性 □其他控管方法：
2.2 網路安全防護			
2.2.1	建立惡意中繼站黑名單	□適用 □不適用 說明：	□建立惡意中繼站黑名單 □其他：
2.2.2	網路設備紀錄檔（log）分析	□適用 □不適用 說明：	□內部對外開放服務連線 □內對外連線事件 □異常高傳輸量情形 □非上班時間之連線情形 □內部是否有黑名單連線情形 □其他：
2.2.3	流量封包側錄	□適用 □不適用 說明：	□網路封包異常連線 □異常 DNS Server 查詢 □惡意 IP □內部連接中繼站 □其他：
2.2.4	加強縱深防禦	□適用 □不適用 說明：	□安裝 IDS/IPS □安裝 WAF □建立 DMZ 緩衝區 □垃圾郵件過濾閘道病毒過濾閘道 □其他：
2.2.5	企業網段管理	□適用 □不適用 說明：	□重要系統網段獨立測試 □正式環境網段與開發測試網段分離 □測試平台禁止真實資料使用 □其他：
2.2.6	定期網頁弱掃、滲透測試 建議每 12 個月至少 1 次	□適用 □不適用 說明：	□網頁弱掃頻率：1 年至少 1 次 □滲透測試頻率：1 年至少 1 次 □其他：
2.3 電腦安全防護			
2.3.1	關閉未使用服務或具風險	□適用	□關閉未使用的 TLS 舊版本

	之 Port 在不影響服務正常運作的情況下，建議 TLS 可升級至最新版，並關閉舊版本	□不適用 說明：	□關閉 FTP，升級為 SFTP □關閉 Telnet，升級為 ssh □其他：
2.3.2	密碼政策實施	□適用 □不適用 說明：	□公司端伺服器最少 12 碼 □使用者端伺服器最少 8 碼 □英文大寫、英文小寫、阿拉伯數字、特殊符號至少四選三 □密碼更新至少 90 天更新 □訂定密碼鎖定原則： □其他：
2.3.3	建立系統及資料備援	□適用 □不適用 說明：	□建立系統備援 □建立資料備援 □其他：
2.3.4	定期主機弱掃、惡意程式檢測 建議每 12 個月至少 1 次	□適用 □不適用 說明：	□主機弱掃頻率：1 年至少 1 次 □惡意程式檢測頻率：1 年至少 1 次 □其他：
2.3.5	定期軟體更新 檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新狀態	□適用 □不適用 說明：	□更新頻率： □更新軟體內容包含： □其他：
2.4 資訊系統開發資安防護			
2.4.1	設計階段（Design） 對外網站服務的資安威脅可參考 OWASP TOP 10（十大網路應用系統安全弱點），於設計階段考量資安威脅	□適用 □不適用 說明：	□分析程式對外服務於資安構面是否有風險 □分析程式內部登入於資安構面是否有風險 □於「威脅建模」(Threat Modeling)逐一列出 □其他：
2.4.2	開發實作階段（Implementation） 應避免常見弱點及發展控制措施	□適用 □不適用 說明：	□透過 HTTPS 傳輸加密 □對稱或非對稱式加密資料庫 □其他：
2.4.3	驗證測試階段（Verification）	□適用 □不適用 說明：	□源碼檢測(靜態分析) □弱點掃描(動態分析) □滲透測試(動態分析) □其他：

2.4.4	部署維運階段（Deployment & Maintenance） 透過版本控制工具，掌握版本是否為最新版，並隨時更新版本、修補漏洞，以維持版本的最佳化	□適用 □不適用 說明：	□更新版本 □修補漏洞 □其他：
2.5 資料安全管理			
2.5.1	資料傳輸	□適用 □不適用 說明：	□IT 系統遠端存取連線軟體升級至企業版本 □SQL（結構化查詢語言）更新至最新版 □個資透過 API 傳輸時做有效加密、隱碼遮罩 □要求個資提供方透過 API 傳輸時，做有效加密及隱碼遮罩 □其他：
2.5.2	資料庫防護	□適用 □不適用 說明：	□系統內採用加解密機制存取設定資料 □資料庫、資料表內個資採用加解密機制存取資料 □增設存取 log 紀錄 □其他：
2.6 系統存取控制			
2.6.1	加強帳號註冊或註銷等權限管理	□適用 □不適用 說明：	□帳號最低權限原則 □不共用帳號 □其他：
2.6.2	於系統中布建使用者身分配置程序	□適用 □不適用 說明：	□於系統中布建使用者身分配置程序 □其他：
2.6.3	管理使用者密碼資訊及特權存取權限應被限制與管理	□適用 □不適用 說明：	□限制與管理使用者存取權限 □其他：
2.6.4	定期檢視使用者權限	□適用 □不適用 說明：	□半年至少 1 次檢視使用者權限 □1 年至少____次檢視使用者權限 □其他：
2.6.5	客戶登入後台之管控	□適用 □不適用	□協助客戶強化登入後台資料庫密碼複雜度

		說明：	□協助客戶強化登入後台資料庫採取多因子認證 □限縮客戶有權限進入後台系統（包含下載權限）之人數 □縮短客戶帳號的登入閒置時間，並於閒置過久時強制登出 □其他：
2.7 系統維護			
2.7.1	不於非上班時間處理客戶突發問題 以確保所有系統操作皆由公司 IP 進行	□適用 □不適用 說明：	□採取_____措施使員工皆由公司 IP 進行系統操作 □其他：
2.7.2	第三方資安健檢	□適用 □不適用 說明：	□定期由第三方資安廠商執行資安健檢 □佈署端點防護軟體 □其他：
2.7.3	發現的資訊服務系統或網站平台的弱點列表及控制措施	□適用 □不適用 說明：	□自主及尋求第三方協助發現的資訊服務系統或網站平台的弱點列表及控制措施 □提出預防或避免攻擊之作法供線上驗證 □其他：
2.8 人員資安認知			
2.8.1	人員資安職能訓練	□適用 □不適用 說明：	□規劃訓練藍圖 □辦理訓練頻率： □其他：
2.8.2	定期電子郵件社交工程演練	□適用 □不適用 說明：	□演練頻率：每半年至少 1 次 □演練內容： □其他：
3.法遵面			
3.1 法規要求事項之識別			
3.1.1	個人資料保護法及個人資料保護法施行細則	□適用 個人資料保護法及個人資料保護法施行細則	□個人資料保護法 □個人資料保護法施行細則
3.1.2	數位經濟相關產業個人資料檔案安全維護管理辦法	□適用	□數位經濟相關產業個人資料檔案安全維護管理辦法

3.1.3	委託者主管機關之相關法令規範 例如：經濟部商業發展署法令、衛生福利部法令、教育部法令	□適用 數位經濟相關產業個人資料檔案安全維護管理辦法第 19 條第 2 項	□《綜合商品零售業個人資料檔案安全維護管理辦法》 □《交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法》 □《社會福利機構個人資料檔案安全維護計畫實施辦法》 □《短期補習班個人資料檔案安全維護計畫實施辦法》 □其他：
3.2 契約要求事項之識別			
3.2.1	定義所提供 ERP 服務的安全使用環境 於資訊安全文件中敘明資訊服務系統的安全使用環境，應配合採行哪些資訊安全配套措施或工具，以及資料透過 API 傳輸及存取過程之資安防護策略	□適用 □不適用 說明：	□資訊安全文件中敘明資訊服務系統安全使用環境 □資訊安全配套措施： □資訊安全配套工具： □資料傳輸及存取過程之資安防護策略： □其他：
3.2.2	資服業者之委託客戶義務	□適用 □不適用 說明：	□一年___次更新各式系統及軟體版本 □配合加裝指定之資訊安全配套措施或工具 □客戶自建伺服器者之連接加密等級 □客戶之電腦設備不可安裝非法軟體 □避免多人共用後臺登入之帳密 □離開電腦或下班時應從後臺登出 □一周___次針對登入後臺電腦使用掃毒 □一年___次社交工程演練 □其他：
3.2.3	資服業者端義務	□適用 □不適用 說明：	□確保網頁安全（SSL 加密） □設計具加密功能的通道使客戶傳輸機敏資料

			□設計傳輸機敏資料時隱碼（遮罩）不必要資訊 □管控客戶存取權限 □一年___次做社交工程演練 □其他：
3.2.4	租用雲端主機時釐清責任	□適用 □不適用 說明：	□釐清連接架構 □確認資料存放和保護管理責任分配 □其他：
4.作業流程面			
4.1 控制措施			
4.1.1	控制措施 四大控制主題（組織、人員、實體與技術）	□適用 □不適用 說明：	□逐步承諾內容： □全部承諾
4.2 資訊安全管理的四階文件			
4.2.1	第一階文件：安全手冊 最高指導文件	□適用 □不適用 說明：	□資訊安全政策 □ISO27001 適用性聲明 □其他國際標準之適用性聲明
4.2.2	第二階文件：管理辦法 企業資訊安全管理制度文件化	□適用 □不適用 說明：	□ □
4.2.3	第三階文件：作業程序 規定標準作業細節	□適用 □不適用 說明：	□ □
4.2.4	第四階文件：紀錄表單 作業流程實際作業	□適用 □不適用 說明：	□ □
5.持續與改善			
5.1 紀錄保存			
5.1.1	導入日誌分析系統與事件反應機制 用以作為存錄與監控，以識別、蒐集、獲取及保存可作為證據之資訊	□適用 □不適用 說明：	□導入日誌分析系統 □導入事件反應機制 □其他：
5.1.2	使用紀錄及軌跡資料證據保存	□適用 □不適用 說明：	□紀錄資料使用紀錄 □紀錄自動化機器設備之軌跡資料

			□落實執行資訊安全管理措施之證據 □其他：
5.2 檢查稽核			
5.2.1	內部資安稽核機制 一年至少一次	□適用 □不適用 說明：	□1 年至少____次內部資安稽核 □提出評估報告 □採行改善機制： □其他：
5.2.2	第三方資安稽核驗證或檢測	□適用 □不適用 說明：	□委請第三方資安稽核 □委請第三方驗證機構進行資安稽核 □委託資安公司進行資安健檢並提出檢測報告 □其他
5.3 持續改善措施			
5.3.1	持續改善措施	□適用 □不適用 說明：	□以 PDCA 之政策說明進行資訊安全政策之持續與改善 □討論會議製作書面紀錄以為佐證 □其他：