**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**

113年11月1日 6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。

1. **配置管理人員（成立個資小組）及相當資源  
   （下圖為舉例，請公司撰寫總負責人及相關管理人員職稱、姓名、執掌等，亦可製作公司自己的小組組織圖）**

**職稱及姓名：**技安 專案管理師

**工作職掌：**

1. 本公司安全維護計畫、個人資料保護政策之訂定及修正、監督執行、檢查
2. 個資保護業務之協調聯繫
3. 本公司個資事故總連絡窗口

**個資保護總負責人(召集人)**

**個資管理專職/責人員**

資訊部

**資訊安全主管**

○○部

**單位個資管理專員**

人資處

**單位個資管理專員**

**職稱及姓名：**小叮噹 總經理

**工作職掌：**

1. 本公司個資安全維護措施之協調與推動
2. 檢驗本公司個資安全防護措施佈署的執行及規劃所需資源
3. 核准本公司個資安全執行之資源需求

**職稱及姓名：**宜靜 人資管理師

**工作職掌：**

1. 人資處個資安全維護措施推動及執行
2. 人資處個資事故連絡窗口

**職稱及姓名：**大雄 資料分析師

**工作職掌：**

1. OO部個資安全維護措施推動及執行
2. OO部個資事故連絡窗口

**職稱及姓名：**阿福 技術副總

**工作職掌：**

1. 本公司系統資安政策之規劃及執行
2. 本公司資訊系統事故調查及改善
3. **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：
5. 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）
6. 事故通報個資聯絡窗口： （個資管理專責人員：技安）
7. 緊急應變程序依照本計畫第五點所列之內容進行。
8. 監督委外廠商依照本計畫第十三點所列內容進行。
9. 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。
10. **清查（盤點）及界定個人資料之範圍**
11. **清查（盤點）及界定頻率： 每年 進行清查盤點及界定一次。**
12. **蒐集、處理或利用個資之屬性**

■所屬人員（含員工、業務、兼職、派遣、顧問、股東等人員）

■消費者（含代管或暫存）

■廠商客戶聯繫窗口

■供應商、承包商聯繫窗口

1. **個資盤點方式（下表舉例，請公司製作自己的表）**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 業務流程/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 | 處理及利用軌跡紀錄存放位置 |
| 001-1  員工基本資料 | 人事管理(勞工名卡) | 姓名、地址、電話、身份證字號 | 聯繫員工、保險 | 台灣地區 | 離職後5年(勞動基準法第7條) | OOO筆 | OO系統之資料處理及利用行為之LOG紀錄 |
| 001-2  員工薪資資料 | 給付薪資 | 金融帳戶、薪資、獎金、勞健保 | 給付薪資 | 台灣地區 | 離職後5年(勞動基準法第7條) | OOO筆 | OO系統之資料處理及利用行為之LOG紀錄 |
| 001-3  員工體檢資料 | 確認員工安全衛生 | 健康檢查資料 | 確認員工安全衛生 | 台灣地區 | 7年(職安法+勞工健康保護規則) | OOO筆 | OO系統之資料處理及利用行為之LOG紀錄 |
| 002供應商聯絡資料 | 聯繫用途、訂定契約 | 姓名、地址、電話、電子郵件 | 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 | OO系統之資料處理及利用行為之LOG紀錄 |
| 003客戶聯繫資料 | 聯繫用途、訂定契約 | 姓名、地址、電話、電子郵件 | 行銷及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 | OO系統之資料處理及利用行為之LOG紀錄 |
| 004客戶之消費者資料 | 1、資（通）訊系統、資料庫或伺服器代管  2、維護系統  3、資料暫存於系統內 | 姓名、地址、電話、電子郵件、訂單、信用卡號、電子發票條碼 | 1、受託管理(或/及儲存)客戶之消費者資料  2、維護時接觸  3、受託暫存 | 伺服器於台灣地區  (或雲端伺服器之OO地區資料中心) | 10天 | OOO筆  (或僅代管伺服器無法控制資料) | OO系統之資料處理及利用行為之LOG紀錄 |

1. **個人資料之風險評估及管理機制**
2. **評估頻率： 每年 進行評估一次。**
3. **風險評估表（下表舉例，請公司製作自己的表）**

【註：業者可評估資料價值及公司規模以投入相應成本採取風險處理對策】

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 業務流程/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 | 作業情境及內容 | 可能風險類型 | 風險處理對策 |
| 001員工資料 | 1 | 2 | 3 | OOO筆 | 例：儲存資料 | 儲存空間未設定存取權限，以致全體員工皆能存取他人健檢資料 | 資料庫權限設定 |
| 002供應商聯絡資料 | 1 | 1 | 2 | OOO筆 | 例：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 |
| 003客戶聯繫資料 | 1 | 1 | 2 | OOO筆 | 例：傳輸(Email) | 行銷時客戶Email未密件副本 | 加強員工教育訓練 |
| 004客戶之消費者資料 | 2 | 3 | 5 | OOO筆  (或僅代管伺服器無法控制資料) | 例：  1、代管伺服器  2、外部傳送(串接第三方系統) | 1、系統之網頁版登入功能有漏洞  2、串接渠道協定有漏洞 | 1、尋找漏洞修正協定  2、傳輸資料雙重隱碼(SSL加密、資料隱碼) |

1. **風險類型及預訂風險對策（下表舉例，請公司製作自己的表）**

|  |  |  |  |
| --- | --- | --- | --- |
| **作業情境** | **作業內容** | **可能風險類型** | **預計風險處理對策** |
| 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 |

1. **事故之預防、通報及應變機制**
2. **事故應變流程圖（下圖舉例，請公司製作自己的圖）**

「發生個資事故」後，通報事故通報個資聯絡窗口、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小時內通報主管機關數位發展部並配合調查。【註：若事故已由媒體報導，建議於24小時內通報主管機關】
2. 通知當事人：初步查明後立即以適當方式通知當事人，使當事人知悉個資事故及已採取之因應措施。
3. 通知客戶：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。【註：公司有提供代管伺服器、代維運系統、提供SaaS服務者，或者系統雖賣斷但同時有多家客戶發生個資事故時，應訂定通知客戶之流程】
4. 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。

通報窗口：個資管理專責人員

**發現個資**

**事件**

**通報個資**

**小組**

**啟動應變程序**

4小時內內

**通報**

**主管機關**

72小時內

(重大矚目案件24小時內)

**通知客戶**

**通知當事人**

**事故排除**

**採取改善措施、後續追蹤**

立即

通知

使當事人知悉個資事故、已採取的因應措施

**配合主管機關調查**

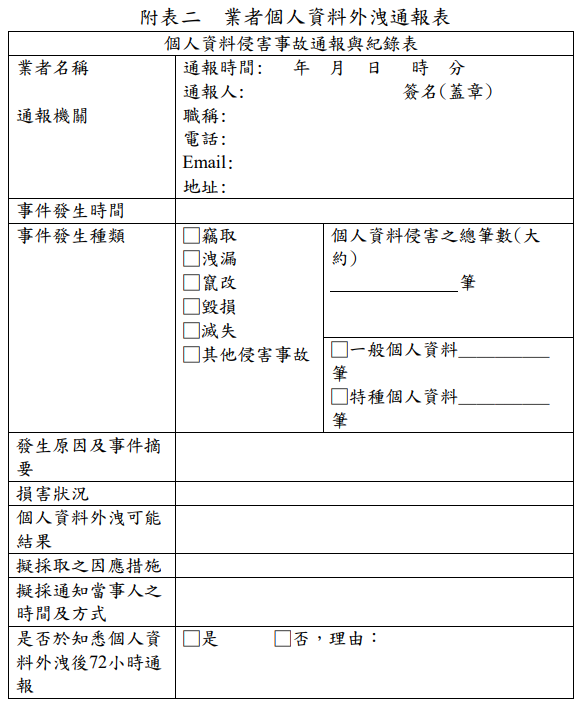
**結案**

例如：尋找惡意程式並刪除、立刻限制國外IP存取等

個資管理專責人員啟動程序

主管機關：數位發展部

1. **事故通報**
2. 通報時點：知悉發生事故72小時內。【註：若事故已由媒體報導，建議於24小時內通報主管機關】
3. 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。
4. 通報對象：數位發展部。電話：02-23808390；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。（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



1. **通知當事人**
2. 通知時點：自知悉時起即初步查明，並立即以適當方式通知當事人。
3. 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。
4. 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。
5. 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。
6. **通知客戶**【註：公司有提供代管伺服器、代維運系統、提供SaaS服務者，或者系統雖賣斷但同時有多家客戶發生個資事故時，應訂定通知客戶之流程】
7. 通知時點：自知悉時起即應盡速通知。
8. 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。
9. 通知內容：使客戶知悉個資遭外洩或竊取、已採取哪些應對及修補措施。
10. 通知方式：以簡訊、電子郵件等其他足以使客戶知悉或可得知悉之方式。
11. **個人資料蒐集、處理及利用之內部管理程序**
12. **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：**
13. **特定目的**
14. 利用個資時符合蒐集時之利用目的。
15. 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。

1. **法律依據**
2. 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。】
3. 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。
4. **告知當事人**
5. 告知個資當事人，符合個資法第8、9條之規定
6. 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。
7. 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。
8. 符合免為告知之情形
9. 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。
10. 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。
11. **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。

1. **國際／境外傳輸之限制、告知**

本公司□未進行個人資料國際傳輸。

本公司□有個人資料國際傳輸，將依個資相關規範進行以下事宜：

1. 基於 等業務行為。將個人資料國際傳輸於 等地區。【註：業務行為例如員工資料傳輸於國外母公司伺服器，或客戶資料儲存於雲端服務業者之境外資料中心。地點請寫國名或地區】
2. 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。
3. 透過 等方式告知當事人其個人資料所將國際傳輸之區域。【註：例如與客戶之契約、隱私權政策】
4. 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。
5. **定期檢視個人資料蒐集之特定目的是否已消失或期限是否已屆滿**
6. **每半年** 定期利用個資盤點表檢視個人資料蒐集之特定目的是否已消失，或期限是否已屆滿。【註：通常每半年或1年】
7. 個人資料之特定目的消失或期限屆滿時，依個資法第11條第3項規定處理：

* 主動刪除、停止處理及停止利用該個人資料。
* 因法規規定、執行職（業）務所必須，或經當事人書面同意者，可不刪除、停止處理或利用。但應於個資盤點表中寫明特定目的消失或期限屆滿時，不刪除、停止處理或停止利用之事由。

1. **受理當事人請求權利之程序**
2. **受理內容**
3. 拒絕行銷之處理程序
4. 受理當事人行使個資法第3條權利之程序
5. 受理個資更正之程序
6. **拒絕行銷受理方式**：
7. 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。
8. 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。
9. 提供當事人免費、快速、容易表達之簡便方式。
10. **當事人行使個資法第3條權利受理方式**：
11. 告知當事人得依個資法第3條規定得行使之權利及方式
12. 至少與蒐集當事人個資相同之方式、管道、難易度相同。
13. 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。

1. **個資更正受理方式：**
2. 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。
3. 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。
4. 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。】
5. 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。
6. **當事人請求權利之受理程序流程圖：**

**（下圖舉例，請公司製作自己的圖）**

**受理**

**當事人請求流程及處理程序**

**拒絕行銷**

當事人當場表示拒絕行銷時之受理方式

**行使個資法第3條權利**

**個資更正**

**當事人請求**

**受理方式**

**內部處理程序**

**銷售人員：**正在行銷時立即停止行銷，並傳達個資保管權責人員

至少與蒐集個資相同之管道，或透過網站申請等受理方式

**個資保管權責人員：**依當事人要求刪除，或註記停止利用

**聯繫窗口：**回復當事人已受理，並傳達給個資保管權責人員

提供客服電話、客服email、網站申請等受理方式

**個資保管權責人員：**依當事人要求處理，並回復處理情形

**聯繫窗口：**回復當事人已受理，並傳達給個資保管權責人員

**個資保管權責人員：**依當事人提供之資訊更正，並回復處理情形

**聯繫窗口：**回復當事人已受理，並傳達給個資保管權責人員

首次行銷時提供免費電話、客服email或網站申請等受理方式

1. **資料安全管理**
   * 1. **本公司提供之 開店平台 系統服務，自行、或協助客戶蒐集、處理或利用個人資料時（例如代管伺服器、代維運系統、提供SaaS服務等），採取以下資料安全管理措施：**【註：不適用者（例如賣斷系統產品），本項目可不填寫】
2. 加密：個人資料有加密之必要時，於 **儲存於資料庫** 時採取 **AES256、TLS 1.3以上** 等加密措施。且解密金鑰與加密資料應存放於不同位置。
3. 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。且備份區儲存位置應與正式區及測試區進行隔離。
4. 傳輸安全：透過 **透過API** 進行資料傳輸時，採取**SSL傳輸加密機制、AES256加密機制** 之安全措施。
5. 外部網路入侵對策：本公司■有□無向客戶提供主機（代）管理服務

■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 **每半年** 定期更新一次。【註：通常每3個月、半年或1年】【註：若未向客戶提供主機（代）管理服務者，本項目可不填寫】

■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 **每半年** 定期更新一次。【註：通常每3個月、半年或1年】

□其他入侵偵測設備： ，並 定期更新一次。

1. 異常存取資料行為之監控及因應演練：
   1. 異常行為之監控

■伺服器內設置異常登入行為監控設備。【註：若未向客戶提供主機（代）管理服務者，本項目可不填寫】

■系統內設置異常存取資料行為監控設備。

* 1. 異常行為因應演練： **每1年** 定期演練異常存取資料行為因應機制。【註：通常每半年或1年】

1. 檢測系統漏洞及修補：
   1. 開發之資訊服務系統產品提供給客戶前，應至少進行**1** 次【註：通常至少1次】進行源碼掃描檢測系統漏洞，並修補漏洞至無中風險及高風險漏洞。
   2. 若與客戶訂有維護契約或（代）管理系統時， **每1年** 【註：通常每半年或1年】定期一次 透過系統網站弱點掃描、主機弱點掃描 檢測伺服器及相關系統漏洞，並修補漏洞至無中風險及高風險漏洞。
2. 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1年** 定期執行惡意程式檢測一次。【註：通常每半年或1年】
3. 密碼及認證機制：

■密碼【註：帳號及密碼須符合一定之複雜度，並建議限制帳號數量、變更頻率縮短、限制特定IP登入等】

■其他認證機制：**雙因子認證**【註：公司開發產品實際需求，例如雙因子認證、多因子認證、生物識別等】

1. 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。
2. 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。
3. 定期檢查： **每1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。【註：通常每半年或1年】
4. 個資隱碼：針對系統或伺服器之 **資料庫儲存資料、API傳輸個資、前台訂單查詢** 之個資使用情境，採行 **資料庫內資料加密、SSL傳輸加密機制、前台使用者介面顯示資料之隱碼機制** 個資之隱碼機制。
5. 其他資料安全措施： 【註：若有無上述情形，可自行填寫】
   * 1. **本公司產品開發政策**（以下內容為舉例）

**本公司提供之 開店平台 系統服務（例如代管伺服器、代維運系統、提供SaaS服務等），採取以下產品開發政策：**【註：不適用者（例如賣斷系統產品），建請改至附錄填寫】

【註：建議公司參考SSDLC訂定產品開發政策（資安部分），並檢視是否符合數位經濟相關產業個人資料檔案安全維護管理辦法及客戶應適用之個資相關規範。】

1. **需求階段**
   1. 系統防護需求分級。
   2. 遵守數位經濟相關產業個人資料檔案安全維護管理辦法。

* 資料庫內資料加密。
* 傳輸資料時採取安全措施(如SSL傳輸協定)。
* 系統安裝應用程式防火牆。
* 系統內有異常存取資料行為監控機制(如LOG機制、異常預警機制)。
* 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系統（如出廠前應至少進行一次源碼掃描及弱點掃描，出廠後定期檢測漏洞及修補、版更）。
* 系統應建置使用者驗證機制(如強密碼、雙因子驗證等) 。
* 資通系統進行測試時應避免使用真實個人資料。
* 系統前台介面應建立隱碼機制。
  1. 遵守客戶應適用之個資相關規範

1. **設計階段（Design）**
2. 對外網站服務的資安威脅參考OWASP TOP 10，於設計階段考量資安威脅。
3. 進行「威脅建模」(Threat Modeling)分析，分析程式對外服務及內部登入於資安構面是否有風險。
4. **開發實作階段（Implementation）**
5. 預防OWASP TOP 10常見漏洞。
6. 透過HTTPS傳輸加密。
7. 對稱或非對稱式加密資料庫。
8. 建置權限控管。
9. 建置異常存取監控機制及預警機制。
10. **驗證測試階段（Verification）**
11. 至少進行1次源碼檢測(靜態分析)。
12. 至少進行1次弱點掃描或滲透測試(動態分析)。
13. **安裝部署及維運階段（Deployment & Maintenance）**
14. 刪除安裝用帳號或修改安裝用帳號之密碼。
15. 文件記錄安裝過程，並經由主管或稽核小組確認。
16. 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。（賣斷系統後若仍有維護契約時，應對系統進行弱點掃描確保系統安全性）
17. 確認異常行為監控機制及預警機制是否正常執行。
18. 落實備份機制。
    * 1. **本公司之公司OA區電腦、共用區等設備，採取以下資料安全管理措施：**
19. 加密：儲存於 **人資管理系統、客戶管理系統資料庫** 之資料採取 **AES256** 等加密措施。且解密金鑰與加密資料應存放於不同位置。
20. 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。且備份區儲存位置應與正式區及測試區進行隔離。
21. 傳輸安全： **客戶管理系統資料庫** 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。
22. 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。【註：通常每3個月、半年或1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**3個月**定期更新一次。【註：通常每3個月、半年或1年】

■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。【註：通常每3個月、半年或1年】

■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。【註：通常每半年或1年】

□其他入侵偵測設備： ，並 (時間)一次定期更新一次。

1. 異常存取資料行為之監控及因應演練：
   1. 異常行為之監控

■伺服器內設置異常登入行為監控設備。

■系統內設置異常存取資料行為監控設備。

* 1. 異常行為因應演練： **每1年** 定期演練異常存取資料行為因應機制。【註：通常每半年或1年】

1. 檢測系統漏洞及修補： **每年** 【註：通常每半年或一年】定期一次透過 **網站弱點掃描、主機弱點掃描** 檢測伺服器及相關系統漏洞，並修補漏洞至無中風險及高風險漏洞。
2. 防毒軟體及惡意程式檢測：
3. 設備及系統隨時更新及執行防毒軟體。
4. **每年** 定期執行惡意程式檢測一次。
5. 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**

1. 避免利用真實個資測試：
2. 處理個資之資通系統進行測試時避免使用真實個資。
3. 使用真實個資者，應訂定使用規範。
4. 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。
5. 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。【註：通常每半年或1年】
6. 個資隱碼：針對系統或伺服器之 **資料庫儲存資料、API傳輸個資、前台使用者介面查詢** 之個資使用情境，採行 **資料庫內資料加密、SSL傳輸加密機制、前台使用者介面顯示資料之隱碼機制** 個資之隱碼機制。
7. 其他資料安全措施： 【註：若有無上述情形，可自行填寫】
8. **人員安全管理**
9. 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**
10. 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**
11. 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：

1. 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**
2. **設備安全管理**
3. 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：　**如端點防護**

■採取儲放環境安全管理措施：　**如檔案室環境規則、共用區存取規則**

□其他：

1. 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：**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**
2. 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：　**如檔案室門禁管制**
3. 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：　**如提供新版本之資料及軟硬體時，繳回或刪除舊版本**
4. **個資保護認知宣導及教育訓練**
5. 定期舉辦全體員工ㄧ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

■個資保護及資安意識

□社交工程演練或辨識社交工程之教學

□其他

1. 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。
2. 資訊人員定期參加特殊訓練， **每年** 至少一次。
3. 實施之佐證紀錄

■簽到簽退

■製作會議紀錄

■課後評量機制

□其他佐證方式

1. **使用紀錄、軌跡資料及證據保存**
2. **個資之蒐集、處理或利用紀錄**
3. 公司OA區電腦、共用區等設備
   1. 保存方法：　**電子資料、紙本紀錄**
   2. 保存地點：　**電子資料存於本公司機房自行管理之伺服器、紙本紀錄存放檔案櫃**
   3. 保存期限：　 **5年**
4. 本公司為提供客戶服務所（代）管理之系統
5. 保存方法：　**電子資料存於本公司租用之AWS雲端伺服器**
6. 保存地點：　**電子資料存於本公司租用之AWS雲端伺服器**
7. 保存期限：　 **5年**
8. **自動化機器設備之軌跡資料**
9. 公司OA區電腦、共用區等設備
10. 保存方法：　**電子資料**
11. 保存地點：　**電子資料存於本公司機房自行管理之伺服器**
12. 保存期限：　 **5年**
13. 本公司為提供客戶服務所（代）管理之系統
14. 保存方法： **電子資料**
15. 保存地點：　**電子資料存於本公司租用之AWS雲端伺服器**
16. 保存期限：　 **5年**
17. **落實執行個人資料檔案安全維護計畫之證據**
18. 保存方法：　**電子資料、紙本紀錄**
19. 保存地點：　**電子資料存於本公司機房自行管理之伺服器、紙本紀錄存放檔案櫃**
20. 保存期限：　**5年**
21. **資料安全稽核**

**本公司資料安全稽核機制如下：**

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

1. 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

1. 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
2. **檢查執行頻率**

**本公司為：**

□資本額1000萬元以下或保有個資5000筆以下者，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

1. **稽核範圍**
2. **本公司所有個資安全維護措施**
   * + - 配置管理之人員及相當資源
       - 界定個人資料之範圍（並檢查是否定期盤點）
       - 個人資料之風險評估及管理機制（並檢查是否定期評估）
       - 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（並檢查是否定期評估檢視個資蒐集目的是否已消失）
       - 資料安全管理措施（並檢查是否定期更新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）
       - 人員安全管理措施（並檢查是否定期檢視個資存取權限）
       - 認知宣導及教育訓練（並檢查是否定期實施全體員工教育訓練、代表人及管理人員教育訓練）
       - 設備安全管理
       - 資料安全稽核機制（並檢查是否定期稽核或自我檢查）
       - 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（並檢查是否定期檢視或修正安全維護計畫）
3. **其他稽核內容**：　產品開發政策
4. **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。
7. **業務終止後個人資料處理方法**
8. **人員離職時之資料返還**
9. 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。
10. 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。
11. **因業務終止而銷毀證據保存**
12. **銷毀**
13. 銷毀之方法： 。
14. 銷毀時間、地點及證明銷毀之記錄方式： 。
15. **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。
16. **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。
17. **上述銷毀、移轉或刪除等紀錄，應保留至少5年。**
18. **個人資料安全維護之整體持續改善**
19. **安全維護計畫未落實執行時應採取矯正預防措施**
20. 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。
21. 評估消除缺失項目所須採取的措施，並實際執行。
22. 審查所有已採取的矯正措施的有效性。
23. 將矯正措施更新於本計畫。
24. 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。
25. **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：本公司產品開發政策及系統安裝政策（資安維護部分）**

【註：若公司從事開發系統或代理系統，且透過銷售賣斷系統，建議公司參考SSDLC訂定產品開發政策（資安部分），及訂定系統安裝政策，並檢視是否符合個資法及客戶應適用之個資相關規範，並可參考數位經濟相關產業個人資料檔案安全維護管理辦法。】（以下內容為舉例）

1. **需求階段**
2. 系統防護需求分級。
3. 遵守數位經濟相關產業個人資料檔案安全維護管理辦法。

* 資料庫內資料加密。
* 傳輸資料時採取安全措施(如SSL傳輸協定)。
* 系統安裝應用程式防火牆。
* 系統內有異常存取資料行為監控機制(如LOG機制、異常預警機制)。
* 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系統（如出廠前應至少進行一次源碼掃描及弱點掃描，出廠後定期檢測漏洞及修補、版更）。
* 系統應建置使用者驗證機制(如強密碼、雙因子驗證等) 。
* 資通系統進行測試時應避免使用真實個人資料。
* 系統前台介面應建立隱碼機制。

1. 遵守客戶應適用之個資相關規範
2. **設計階段（Design）**
3. 對外網站服務的資安威脅參考OWASP TOP 10，於設計階段考量資安威脅。
4. 進行「威脅建模」(Threat Modeling)分析，分析程式對外服務及內部登入於資安構面是否有風險。
5. **開發實作階段（Implementation）**
6. 預防OWASP TOP 10常見漏洞。
7. 透過HTTPS傳輸加密。
8. 對稱或非對稱式加密資料庫。
9. 建置權限控管。
10. 建置異常存取監控機制及預警機制。
11. **驗證測試階段（Verification）**
12. 至少進行1次源碼檢測(靜態分析)。
13. 至少進行1次弱點掃描或滲透測試(動態分析)。
14. **安裝部署及維運階段（Deployment & Maintenance）**
15. 刪除安裝用帳號或修改安裝用帳號之密碼。
16. 文件記錄安裝過程，並經由主管或稽核小組確認。
17. 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。（賣斷系統後若仍有維護契約時，應對系統進行弱點掃描確保系統安全性）
18. 確認異常行為監控機制及預警機制是否正常執行。
19. 落實備份機制。