



1 目的

1.1 確保本公司落實個人資料之保護及管理，確保本公司在蒐集、處理或利用個人資料時，皆能尊重當事人之權益，並於特定目的之必要範圍內，依誠實信用方法為之，且與蒐集之目的具有正當合理之關聯，因此依據：

1.1.1 本公司個人資料保護最高指導原則【個人資料管理政策】之規劃。

1.1.2 我國【個人資料保護法】(以下簡稱【個資法】)、【個資法施行細則】及其他相關法律，訂定本公司【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】(以下簡稱本計畫及處理方法)，作為本公司個人資料管理體系執行個人資料安全維護措施之規範。

2 適用範圍

本計畫及處理方法適用於：依據本公司【個人資料管理政策】、【個資法】、【個資法施行細則】或其他要求而納入本公司個人資料管理體系之個人資料相關作業(包括蒐集、處理或利用等...)。

3 名詞定義

3.1 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

3.2 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

3.3 蒐集：指以任何方式取得個人資料。

3.4 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

3.5 利用：指將蒐集之個人資料為處理以外之使用。

3.6 當事人：指個人資料之本人。

4 個人資料檔案安全維護管理措施

4.1 管理人員：

4.1.1 配置人數：一人



4.1.2 職責：負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項，並向負責人提出報告。

4.2 預算：每一年新台幣 20 萬元。

4.3 個人資料保護管理政策：遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、篡改、毀損、滅失或洩漏。

5 個人資料之範圍

5.1 特定目的：蒐集之目的在於進行行銷業務、消費者、客戶管理與服務、網路購物及其他電子商務服務及與調查、統計與研究分析。大學光學將藉由加入會員之過程或進行交易之過程來蒐集個人資料。

5.2 客戶個人資料：本計畫所稱之客戶個人資料，除係指客戶姓名、出生年月日、國民身分證統一編號、婚姻、家庭、教育、職業、聯絡方式外及其他以直接或間接方式識別該個人之資料。

5.3 員工個人資料：指姓名、身分證字號、護照號碼、住址及電話號碼、電子郵件與其他聯絡或遞送方式、銀行帳戶、信用狀況、財務資訊與財產狀況等，及其他得以直接或間接識別該個人之資料。

6 風險評估及管理機制

6.1 風險評估

6.1.1 經由本公司電腦下載或外部網路入侵而外洩。

6.1.2 經由接觸書面契約書類而外洩。

6.1.3 員工故意竊取、毀損或洩漏。

6.2 管理機制

6.2.1 藉由使用者代碼、識別密碼設定及文件妥適保管。

6.2.2 定期進行網路資訊安全維護及控管。

6.2.3 加強對員工之管制及設備之強化管理。



7 個人資料蒐集、處理及利用之內部管理措施

7.1 直接向當事人蒐集個人資料時，應明確告知以下事項：

7.1.1 公司(商號)名稱。

7.1.2 蒐集目的。

7.1.3 個人資料之類別。個人資料利用之期間、地區、對象及方式。

7.1.4 當事人依個人資料保護法第三條得行使之權利及方式。

7.2 當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。

7.3 利用個人資料為行銷時，當事人表示拒絕行銷後，應立即停止利用其個人資料行銷。

7.4 客戶表示拒絕行銷或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，連絡窗口為：客服專線電話 0800-747474。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

7.5 負責保管及處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理。

7.6 本公司員工如因其工作執掌相關而須輸出、輸入個人資料時，均須輸入其個人之使用者代碼及密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

7.7 由指定之管理人員定期清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。

7.8 本公司如有委他人（或他公司）蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項。

7.9 所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合規定。

7.10 本公司因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

8 事故之預防、通報及應變機制



8.1 預防：

8.1.1 本公司員工如因其工作執掌而須輸出、輸入個人資料時，均須先登入資訊系統以確認其個人之使用者代碼及密碼，同時在使用範圍及使用權限內為。

8.1.2 加強員工教育宣導，並嚴加管制。

8.2 通報及應變：

8.2.1 發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向公司負責人通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。

8.2.2 對於個人資料遭竊取之客戶，應即以適當方式通知當事人被侵害之事實以及已採取之措施。適當方式得依以言詞、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使當事人知悉或可得悉之方式為之。

8.2.3 針對事故發生原因分析，並研議擬事故應變處理措施避免事故擴大，並採取證據保全措施，避免異動或改變原始磁碟及證據。

9 資料安全管理、人員管理及設備安全管理

9.1 資料安全管理：

9.1.1 電腦存取個人資料之管控：

9.1.1.1 個人資料檔案儲存在電腦硬式磁碟機上者，應在個人電腦設置識別密碼、保護程式密碼及相關安全措施。

9.1.1.2 本公司員工如因其工作執掌相關而須輸出、輸入個人資料時，均於資訊系統登入以確認其個人之使用者代碼及識別密碼及使用權限，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

9.1.1.3 個人資料檔案使用完畢應即退出，不得任其停留於電腦終端機上。

9.1.1.4 定期進行電腦系統防毒、掃毒之必要措施。

9.1.1.5 重要個人資料應另加設管控密碼，非經陳報單位主管核可，並取得密碼者，不得存取。

9.2 紙本資料之保管：

9.2.1 對於紙本客戶資料表應存放於指定檔案櫃中並上鎖，員工非經公司負責人或營業主管同意不得任意複製或影印。

9.2.2 對於記載個人資料之紙本丟棄時，應依「資訊資產管理程序」要求進行銷毀作業。



9.3 人員管理：

- 9.3.1 本公司依業務需求，會適度設定所屬人員(例如主管、非主管人員)不同之權限，以控管其個人資料之情形。
- 9.3.2 本公司員工每 90 天應變更識別密碼 1 次，並於變更識別密碼後始可繼續使用電腦。
- 9.3.3 員工離職或終止僱傭或委任契約時，將立即取消其使用者代碼(帳號)及識別密碼。其所持有之個人資料應辦理交接，不得在外繼續使用，並簽訂保密切結書（如在任職時之相關勞務契約已有所約定時，亦屬之）。
- 9.3.4 本公司員工應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。
- 9.3.5 本公司與員工所簽訂之相關勞務契約或承攬契約均列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後）。

9.4 設備安全管理：

- 9.4.1、建置個人資料之有關電腦設備，資料保有單位應定期保養維護，於保養維護或更新設備時，並應注意資料之備份及相關安全措施。
- 9.4.2 建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。
- 9.4.3 公司應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。
- 9.4.4 本公司對儲存在伺服器上之客戶個人資料檔案每天備份。
- 9.4.5 重要個人資料備份應異地存放，並應置有防火設備及保險箱等防護設備，以防止資料滅失或遭竊取。
- 9.4.6 電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，本公司會對有關設備作適當的資料清除程序。

10 資料安全稽核機制

- 10.1 本公司定期每年辦理個人資料檔案安全維護稽核，查察本公司是否落實本計畫規範事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

- 10.1.1 確認不符合事項之內容及發生原因。
- 10.1.2 提出改善及預防措施方案。



10.1.3 紀錄查察情形及結果。

10.2 前項查察情形及結果應載入稽核報告中，由公司資訊安全主管簽名確認。

11 使用記錄、軌跡資料及證據保存

11.1 本公司將儲存在伺服器上的資料存放於南港辦公室機房，並每日將有關資料進行異地備份儲存。

12 認知宣導及教育訓練

12.1 本公司每年進行個人資料保護法基礎教育宣導及教育訓練至少一次，使員工或所屬之經紀人員知悉應遵守之規定。前述教育宣導及訓練應留存紀錄（例如：簽名冊等文件）。

12.2 對於新進人員應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

13 個人資料安全維護之整體持續改善

13.1 本公司將隨時依據計畫執行狀況，注意相關技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正。

13.2 針對個資安全稽核結果不合法令之虞者，規劃改善與預防措施。

14 業務終止後之個人資料處理方法

14.1 本公司業務終止後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並留存相關紀錄：

14.1.1 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

14.1.2 移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。



大學光學科技股份有限公司

Universal Vision Biotechnology Co., Ltd

文件系統：總部系統

文件編號：U-K-2-116

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

版本：1

頁次：8 of 8

14.1.3 其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

15 實施與修改

本計劃經呈總經理核准後公佈實施，修改時亦同。