華廣生技股份有限公司
個人資料保護實施情形

本公司重視個人資料與隱私權保護，遵循《個人資料保護法》，訂定《個人資料管理政策》及《個人資料檔案安全維護計畫》並建立嚴謹的個資隱私安全管理與防護措施，同時建構健全資料治理制度，執行資料存取管控與檢核機制，確保資料在存取與共享過程中，受到完整保護。適用範圍涵蓋本公司員工、子公司、客戶及供應商。針對營運過程中所涉及之個人資訊蒐集、處理、利用及保護，我們均嚴格遵循政府相關法令規章。此外，本公司每年均進行個資保護宣導，向全體員工公告並再次提醒相關責任與注意事項，以強化員工對個資保護的認知，確保相關制度能確實落實與持續精進。

附件：《個人資料管理政策》、《ISO/IEC 27701 隱私資訊管理系統》、
《個人資料檔案安全維護計畫》

114 年度投入個資保護政策相關量化數據及管理指標如下：

(1). 認證：通過ISO/IEC 27001資訊安全及ISO/IEC 27701個資保護第三方審查，相關資安、個資保護稽核無缺失。

(2). 基於雲端安全發展趨勢，保障產品資訊安全與客戶資料保護，115年變更 ISO/IEC 27001、ISO/IEC 27701驗證範圍，以因應CDMO市場國際化之需求，並通過ISO/IEC 27017(雲服務資訊安全)、ISO/IEC 27018(雲服務個資保護)等稽核驗證。

(3). 客戶滿意度：全年無重大資安事件，無違反客戶資料遺失之投訴案件。

(4). 教育訓練：所有新進員工到職前皆完成資訊安全、個資保護教育訓練課程；全年度共辦理4場次一般員工及專業人員資安(4小時)、個資保護(4小時)教育訓練，受訓人次計有100人以上，每場次均留有考核紀錄；114年度共計執行二次社交工程釣魚郵件測試。

(5). 資料防洩漏(DLP)：導入資料防洩漏(DLP)機制，機密等級以上檔案系統自動加密，保障公司智慧財產安全。

(6). 每月定期召開資安小組會議，檢討與資訊安全、個資保護以及營業秘密有關議題，年底召開管理審查會議，報告全年度資安管理、個資保護工作之成果與指標評估。

(7). 考量公司資安管理機制及措施應可滿足公司營運，並充分展現對於資安、個資保護合規作為，故公司決議暫無須投保資安險，未來將視內外部整體資安、個資保護發展狀況再行決定是否投保。

(8). 於114年完成營業秘密業務檔案盤點及內部稽核作業，加強機密檔案管理機制，落實營業秘密管理制度PDCA循環。

BIONIME

華 廣 生 技 股 份 有 限 公 司

個人資料管理政策聲明

華廣生技股份有限公司 (以下簡稱本公司)秉持落實個人資料保護及管理措施，遵循『個人資料保護法』所述之相關要求及保障個人資料當事人之權利，降低任何因個人資料檔案受侵害事件所可能帶來的衝擊，並持續運作及改善個人資料管理制度，特發布表聲明。

本公司個人資料管理政策聲明如下：

(1) 僅基於合法的特定目的，在確認必要的範圍內處理個人資料。

(2) 僅基於合法目的蒐集最少的必要個人資料。

(3) 僅處理相關且適當的個人資料，並公平且合法地處理之。

(4) 清楚告知當事人，其個人資料將如何被使用及被誰使用。

(5) 維持一份本公司所蒐集、處理及利用的個人資料檔案清冊。

(6) 定期執行隱私衝擊評鑑，採取適當之對策或控制措施，有效降低個人資料檔案遭受損害的風險。

(7) 確保個人資料的正確性，並於必要時進行更新。

(8) 在合於法律、法規的特定目的下保存個人資料。

(9) 尊重並提供當事人對其個人資料依法行使之權利，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、處理或利用及請求刪除等。

(10) 確保所有個人資料檔案的安全。

(11) 僅在有適當充分保護的狀況下，將個人資料進行國際傳輸。

(12) 當個人資料應用於『個人資料保護法』所允許之例外情形時，應確保其適用性與適法性。

(13) 建立與實作個人資料管理制度，落實個人資料管理政策及目標。

表單編號: PF-05-01-01

BIONIME

華 廣 生 技 股 份 有 限 公 司

個人資料管理政策聲明

(14) 於個人資料管理制度運行中，明確界定員工之責任與義務。

(15) 對於委託處理個人資料之分包商採取適當之監督，以確保個人資料處理之安全。

本聲明之頒布，明確宣示維護個人資料管理的重要性，本公司全體員工應確實瞭解此聲明，以維護本公司所有個人資料檔案之安全與永續經營。

制定日期：2019年12月12日

華廣生技股份有限公司

總經理 黃清木 敬上

表單編號: PF-05-01-01

www.tcicgroup.com

管理系統驗證證書

華廣生技股份有限公司
402 台中市南區大慶街二段100號

BIONIME

隱私資訊管理系統
符合下列標準要求

ISO/IEC 27701:2019、CNS 27701:2020

驗證範圍：
全方位血糖管理平台服務及客戶關係管理、客戶服務案件管理以及產品保固之個人資料處理作業，並與適用性聲明(版次9)一致。

驗證位址：
402 台中市南區大慶街二段100號

本證書是基於ISO/IEC 27001證書編號為6-020-2020-ISMS所做的ISO/IEC 27701驗證；獲證單位為PII控制者及處理者。

環奧國際驗證有限公司
證書編號： 5-001-2021-PIMS
初次驗證：2021年03月03日
有效期限：2027年02月07日

台北市，2026年02月06日

TCIC CERTIFIED ISO/IEC 27701 CNS 27701

獲證單位將透過年度追查稽核及每三年的重新驗證稽核，以維持本證書之有效性。

華 廣 生 技 股 份 有 限 公 司

Bionime Corporation

個人資料檔案安全維護計畫

Personal Data File Security Maintenance Plan

壹、 組織及規模

一、 組織型態：股份有限公司。

二、 營業項目：醫療器材批發、生物技術服務、精密儀器批發、醫療器材製造、電信管制射頻器材製造和電信管制射頻器材輸入等業務。

三、 資本額：新台幣10億元整。

四、 代表人(負責人)：黃椿木。

五、 地址：台中市南區大慶街二段100號。

六、 員工人數：約1000人。

貳、 個人資料檔案之安全維護管理措施(計畫內容)

一、 管理人員及資源

(一) 管理人員：

1. 配置人數：2人，並指派擔任個資保護長、個資保護官。
2. 職責：負責規劃、訂定、修正與執行本計畫及業務終止後個人資料處理方法與其他相關事項，並定期向負責人提出報告。

(二) 預算：每年編列資訊安全及個資保護等相關預算約新臺幣1,200萬元。

二、 個人資料之蒐集、處理及利用

(一) 個人資料之蒐集

1. 本公司各單位蒐集個人資料前應確認蒐集、處理個人資料具有特定目的及法定要件，且蒐集內容須與蒐集訂定目的具備合理關聯性。
2. 本公司各單位向當事人蒐集個人資料時，應依據應告知當事人事項，進行告知。

(1) 如符合『個人資料保護法』第 8 條第 2 項規定免告知情形時，則免告知。

(2) 告知的方式得以言詞、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。

3. 本公司各單位蒐集病歷、醫療、基因、性生活、健康檢查及犯罪前科等個人資料時，應“經當事人書面同意”後方得蒐集。

4. 本公司蒐集之個人資料應以達成特定目的必要範圍之最小範圍為原則，所有個人資料蒐集行為應適當控制並予以記錄。

(二) 個人資料之處理

1. 本公司處理個人資料時，應有『個人資料保護法』規定之特定目的並符合特定情形。

2. 本公司各單位於處理個人資料過程中應注意確保其正確性。

(1) 於記錄、輸入、編輯、更正個人資料時，應檢查確認其正確性。

(2) 應主動或依當事人之請求更正或補充之。如因可歸責於本公司之事由，應於更正或補充後，通知曾提供利用之對象。

3. 個人資料之刪除（銷燬）

(1) 本公司各單位應定期檢視個人資料之有效性及可用性，刪除或銷燬過期或無須保留之個人資料。

(2) 本公司各單位保有之個人資料於蒐集之特定目的消失、期限屆滿時，應主動或依當事人之請求刪除或銷燬該個人資料。但因執行業務所必須或經當事人同意者，不在此限。

(3) 本公司各單位於刪除或銷燬個人資料時，應留有審查記錄並確認其執行結果。

(4) 如當事人認為本公司有違反『個人資料保護法』之規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

(三) 個人資料之利用

1. 本公司各單位利用個人資料時，應於蒐集之特定目的必要範圍內為之，如有特定目的外利用之情況，須符合『個人資料保護法』第 20 條之規定。

2. 本公司各單位對於以“經當事人同意”方式蒐集的個人資料，其利用應符合本公司告知事項之內容，包括個人資料利用之期間、地區、對象、方式及其他相關事項。

3. 個人資料之揭露

(1) 本公司各單位揭露個人資料給公務機關執行公務，必須取得公務機關加蓋印信之正式公文函件後始得提供。

(2) 本公司各單位因業務需求須揭露個人資料給第三方時，應：

A. 確認第三者已與本公司簽訂載明雙方個人資料保護權利義務之保密協議書。

B. 確認利用個人資料符合特定目的必要範圍內之利用；於特定目的外利用個人資料時，應檢視是否具備法訂特定目的外利用要件。

C. 確認僅揭露最少內容之個人資料項目。

(3) 向第三方進行個人資料傳遞之紀錄，應予完整留存至少五年。

4. 利用個人資料行銷

(1) 首次行銷時，應提供當事人表示拒絕接受行銷之方式。

(2) 當事人表示拒絕接受行銷時，立即停止利用其個人資料行銷。

(四) 個人資料之停止蒐集、處理、利用

1. 個人資料之蒐集、處理或利用有違法之情事時，本公司各單位應主動或依當事人請求停止蒐集、處理或利用該個人資料。

2. 本公司各單位保有個人資料之正確性有爭議、蒐集之特定目的消失或期限屆滿者，應主動或依當事人之請求停止處理或利用該個人資料。但因執行業務所必須或經當事人同意者，不在此限。

三、 個人資料之範圍及項目

個人資料檔案安全維護計畫
Personal Data File Security Maintenance Plan

(一) 特定目的及類別

1. 特定目的

(1) 人事管理（002）

(2) 公共衛生及傳染病防治（012）

(3) 全民健康保險、勞工保險、農民保險、國民年金保險及其他社會保險（031）

(4) 行銷（040）

(5) 投資管理（044）

(6) 契約、類似契約或其他法律關係事務（069）

(7) 計畫、管制考核與其他研考管理（078）

(8) 食品、藥政管理（080）

(9) 消費者、客戶管理與服務（090）

(10) 消費者保護（091）

(11) 財產保險（093）

(12) 財產管理（094）

(13) 商業與技術資訊（098）

(14) 國內外交流業務（099）

(15) 帳務管理及債權交易業務（104）

(16) 採購與供應管理（107）

(17) 教育或訓練行政（109）

(18) 產學合作（110）

(19) 場所與進出安全管理（116）

(20) 智慧財產、光碟管理及其他相關行政（118）

(21) 貿易推廣及管理（123）

(22) 會計與相關服務（129）

(23) 資(通)訊服務（135）

(24) 資(通)訊與資料庫管理（136）

(25) 資通安全與管理（137）

(26) 僱用與服務管理（145）

(27) 網路購物及其他電子商務服務（148）

(28) 調查、統計與研究分析（157）

(29) 學術研究（159）

(30) 輻射防護（161）

(31) 其他經營合於營業登記項目或組織章程所定之業務（181）

(32) 其他諮詢與顧問服務（182）

2. 類別

(1)C001 辨識個人者：姓名、職稱、住址、工作地址、住家電話號碼、行動電話、即時通帳號、通訊及戶籍地址、相片、電子郵遞地址...等

(2)C002 識別財務者：金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、個人之其他號碼或帳戶...等

(3)C003 政府資料中之辨識者：身分證統一編號、統一證號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼...等

(4)C011 個人描述：年齡、性別、生日、出生地、國籍...等

(5)C012 身體描述：身高、體重、血型...等

(6)C013 習慣：抽菸、喝酒...等

(7)C014 個性：個性等之評述意見...等

(8)C021 家庭情形：結婚有無、配偶姓名、子女人數...等

(9)C023 家庭其他成員之細節：子女、家庭其他成員或親屬、父母...等

(10) C033 移民情形：護照、工作許可文件、居留證明文件、住居或旅行限制、入境之條件及其他相關細節...等

(11) C040 意外或其他事故及有關情形

(12) C051 學校紀錄

(13) C052 資格或技術：學歷資格、專業技術、特別執照、政府職訓機構學習過程、國家考試、考試成績或其他訓練紀錄...等

(14) C054 職業專長：專家、學者、顧問...等

(15) C061 現行之受僱情形：僱主、工作職稱、工作描述、等級、受僱日期、工時、工作地點、產業特性、受僱之條件及期間、與現行僱主有關之以前責任與經驗...等

(16) C062 僱用經過：日期、受僱方式、介紹、僱用期間...等

(17) C063 離職經過：離職之日期、離職之原因、離職之通知及條件...等

(18) C064 工作經驗：以前之僱主、以前之工作、失業之期間及軍中服役情形...等

(19) C065 工作、差勤紀錄：上、下班時間及事假、病假、休假、娩假各項請假紀錄在職紀錄或未上班之理由、考績紀錄、獎懲紀錄、褫奪公權資料...等

(20) C066 健康與安全紀錄：職業疾病、安全、意外紀錄、急救資格、旅外急難救助資訊...等

(21) C068 薪資與預扣款：薪水、工資、佣金、紅利、費用、零用金、福利、借款、繳稅情形、年金之扣繳、工會之會費、工作之基本工資或工資付款之方式、加薪之日期...等

(22) C070 工作管理之細節：現行義務與責任、工作計畫、成本、用人費率、工作分配與期間、工作或特定工作所花費之時間...等

(23) C071 工作之評估細節：工作表現與潛力之評估...等

(24) C072 受訓紀錄：工作必須之訓練與已接受之訓練，已具有之資格或技術...等

(25) C073 安全細節：密碼、安全號碼與授權等級...等

(26) C081 收入、所得、資產與投資：總收入、總所得、賺得之收入、賺得之所得、資產、儲蓄、開始日期與到期日、投資收入、投資所得、資產費用...等

(27) C082 負債與支出：支出總額、租金支出、貸款支出、本票等信用工具支出...等

(28) C083 信用評等：信用等級、財務狀況與等級、收入狀況與等級...等

(29) C084 貸款：貸款類別、貸款契約金額、貸款餘額、初貸日、到期日、應付利息、付款紀錄、擔保之細節...等

(30) C085 外匯交易紀錄

(31) C086 票據信用：支票存款、基本資料、退票資料、拒絕往來資料...等

(32) C087 津貼、福利、贈款

(33) C088 保險細節：保險種類、保險範圍、保險金額、保險期間、到期日、保險費、保險給付...等

(34) C089 社會保險給付、就養給付及其他退休給付：生效日期、付出與

收入之金額、受益人...等

(35) C091 資料主體所取得之財貨或服務：貨物或服務之有關細節、資料主體之貸款或僱用等有關細節...等

(36) C092 資料主體提供之財貨或服務：貨物或服務之有關細節...等

(37) C093 財務交易：收付金額、信用額度、保證人、支付方式、往來紀錄、保證金或其他擔保...等

(38) C101 資料主體之商業活動：商業種類、提供或使用之財貨或服務、商業契約...等

(39) C102 約定或契約：關於交易、商業、法律或其他契約、代理...等

(40) C103 與營業有關之執照：執照之有無、市場交易者之執照、貨車駕駛之執照...等

(41) C111 健康紀錄：檢驗結果、血糖量測記錄...等

(42) C114 交通違規之確定裁判及行政處分：裁判及行政處分之內容、其他與肇事有關之事項...等

(43) C115 其他裁判及行政處分 : 裁判及行政處分之內容、其他相關事項...等

(44) C133 輻射劑量資料：人員之輻射劑量資料...等

(二) 個人資料

本計畫所稱個人資料係指自然人之姓名、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、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、社會活動及其他得以直接或間接方式識別該個人之資料。

四、 人員管理及教育訓練

(一) 人員管理

1. 本公司依業務需求，適度設定所屬員工(例如主管、非主管員工)依不同之權限，控管其個人資料。

2. 本公司員工應妥善保管個人資料之儲存媒體，執行業務時依『個人資料保護法』之規定蒐集、處理及利用個人資料。

3. 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）。

(二) 教育訓練

1. 教育訓練規劃

(1)每年至少執行一次全廠個人資料保護觀念宣導或教育訓練。

(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。

2. 教育訓練內容

包括但不限於：

(1)個人資料保護法及施行細則。

(2)本公司制訂的各項個人資料保護管理作業程序。

(3)個人資料盤點及風險評估。

(4)個人資料外洩事件危機處理應變。

(5)個人資料保護作業內部稽核。

五、 事故之預防、通報及應變機制

(一) 個人資料外洩事件之預防

本公司所有人員在日常管理與營運上，以「計畫-執行-檢視-改善」為基礎，落實資訊安全及『個人資料保護法』相關的規定，以防止個人資料外洩。

(二) 事件通報

1. 本公司所有人員發現疑似員工或病人個人資料外洩事件，應依「資訊安全事故管理程序書」(SP-AG-01)之規定即時通報各受理窗口。

2. 通報受理窗口

(1)外部用戶、消費者、APP用戶等對象，透過客戶客服流程通報。

(2)外部合作伙伴，包括診所、醫院、長照中心與藥局等對象，透過一線接觸的業務人員通報。

(3)公司內部部門等對象：依外洩事件內容選擇IT、IOT進行通報。

(4)網站公告通報窗口：客服單位。

(三) 事故應變

1. 各通報受理窗口於接獲通報後，應依據「資訊安全事故管理程序書」(SP-AG-01)之個資事件分級標準，判定是否為個資外洩事件或異常事件。

2. 經確認為個人資料外洩事故時，應立即採取必要之應變措施以降低或控制損害，並依事件等級通報至緊急應變小組、管理委員會或總召集人。

3. 緊急應變小組組長，應於最短時間內召開緊急應變小組會議，並就相關事務做成決定。

4. 依法於發現事故時起七十二小時內，通報當地主管機關及通知中央主管機關。

5. 依『個人資料保護法』及相關規定通報當事人，期使當事人瞭解相關狀況，並提供後續查詢及協助。

6. 應就事故真實性、外洩資料的數量及範圍進行調查，調查過程應注意證據保全以利日後法律舉證。

7. 判斷事故內容已符合【臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序】時，經報請管理代表及董事長同意後，交公司發言人或代理發言人對外發布訊息。

(四) 檢討改善

緊急應變小組組長應於個人資料外洩事故處理完成後，召開事故檢討會議並擬定改善計劃，以防止類似事故再次發生；必要時，得重新進行風險評估及個人資料管理機制之設計。

六、 設備安全管理

(一) 資訊設備之管理

1. 本公司電腦設備皆安裝合法授權的軟體。
2. 資訊設備應定期進行保養及維護並留有紀錄。

(二) 設備安全措施

1. 建置個人資料之相關電腦設備，應定期保養維護，於保養維護或更新設備時，並注意資料之備份及相關安全措施。
2. 建置個人資料之電腦，不得直接作為公眾查詢之前端工具。
3. 應指派專人管理儲存個人資料之相關電磁紀錄物或媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。
4. 個人資料檔案應定期備份。
5. 重要個人資料備份應異地存放，並應建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。
6. 電腦、自動化設備或其他儲存媒體需報廢汰換或轉作其他用途時，本公司各部門主管應確認該設備所儲存之個人資料是否已確實刪除。
7. 所有儲存媒體在報廢時，必須以消磁、實體破壞或磁碟穿孔等方式，使個人資料無法再次被利用，報廢過程須予以記錄以備日後稽核存證。
8. 如報廢作業委外進行，須事先與承攬廠商簽訂保密協定，以確保個人資料不外洩。

七、 資料安全稽核機制

(一) 本公司定期辦理個人資料檔案安全稽核，查察是否落實本公司制定之個資保護相關程序及規範之事項，針對稽核結果不符合事項及潛在不符合之風險，規劃

改善與預防措施，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：

1. 確認不符合事項之內容及發生原因。
2. 提出改善及預防措施方案。
3. 紀錄查察情形及結果。

(二) 前項查察情形及結果應載入稽核報告中，由管理代表簽名確認。

八、 資料安全管理

(一) 電腦存取個人資料之管控

1. 電腦儲存有個人資料檔案者，應設有密碼保護。
2. 個人資料檔案使用完畢應即退出，不得任其停留於電腦螢幕上。
3. 定期進行電腦系統防毒、掃毒之必要措施。
4. 重要個人資料應設置密碼保護，非經授權不得存取。

(二) 紙本資料之保管

1. 對於各類契約書件及個人資料表應存放於上鎖之公文櫃內，非經部門主管同意或經授權的人，不得任意複製或影印。
2. 對於記載個人資料之紙本丟棄時，應以碎紙設備進行處理。

九、 使用記錄、軌跡資料及證據保存

(一) 本公司必要留存之紀錄與證據之類型包括：書面及電子形式（電子表單、電子郵件、...）檔案。

(二) 必要紀錄、軌跡資料及證據之存取

1. 所有紀錄、軌跡資料及證據皆嚴禁以任何方式新增、更新或刪除。
2. 調閱紀錄、軌跡資料及證據需填寫「重大安全事件電磁紀錄存取申請單」，經總經理核可後，方可調閱或存取。

十、 業務終止後，個人資料處理方法

(三) 資料保存期限

1. 員工在職期間之個人資料，依『勞動基準法』、『個人資料保護法』等規定至少保存至員工離職後五年。
2. 醫療機構上傳至雲端之個人資料，依『醫療法』、『個人資料保護法』等相關規定辦理。
3. 其餘個人資料依據『個人資料保護法』及相關法律規定之保存期限辦理。

(四) 本公司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。

(五) 特定目的消失或被要求刪除之個人資料

1. 如為紙本資料，應以碎紙機或集中送銷的方式予以銷毀。
2. 如為電子檔案，刪除過程須留有記錄。
3. 如為資料庫資料，應確認系統可以完全刪除，並留存紀錄備查。

(六) 特定目的消失或被要求停止處理或利用之個人資料

1. 如為紙本資料，應封存後儲存至具有實體安全防護機制的安全處所，以防止資料遭竊取、毀損或滅失。
2. 如為電子檔案，須使用加密之方式加以封存，密碼應專人保管。
3. 如為資料庫內之個人資料，應將特定資料欄位加以註記並限制存取。

十一、個人資料安全維護之整體持續改善方案

(一) 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訂等事項，檢討本計畫是否合宜，並予必要之修訂。

(二) 針對個資安全稽核結果不符合法令或規定者，應規劃改善與預防措施。