華電聯網股份有限公司
<個人資料安全維護計畫>

第 A 版 2 次

2020 年 06 月 05 日頒行
2024 年 06 月 07 日修訂

修訂內容/紀錄

制/修訂日期	版次	制/修訂內容摘要
2024/06/07	A2	修正敏感與機密等級處理要點出處，以及修正部分詞彙敘述。
2024/01/15	A1	修訂機密等級內容。

目　錄

1. 目的

華電聯網股份有限公司（以下簡稱本公司）為落實個人資料之保護管理，遵循「個人資料保護法」之規定，茲訂定「個人資料檔案安全維護計畫」(以下簡稱「本計畫」)，本計畫之目的，在兼顧個人隱私權的保護及個人資料的合理利用，建立廠商對個人資料蒐集、處理及利用之程序，落實對個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏，並尊重當事人對權利之行使及諮詢。

2. 適用範圍

本公司。

3. 說明

3.1 管理人員及資源

3.1.1 本公司配置一位個資專職人力，同時各單位皆配置一位資安專人，並加強資安人員之培訓（如取得相關專業證照)，提升其協助推動及維護個資保護各項管控措施能力。

3.1.2 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，並向資安暨個資管理代表提出報告。

3.2 個人資料之範圍

3.2.1 特定目的：〇〇一人身保險；〇〇二 人事管理；〇九〇消費者、客戶管理與服務；一〇七採購與供應管理；〇三一全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險；〇五二法人或團體對股東、會員(含股東、會員指派之代表)、董事、監察人、理事、監事或其他成員名冊之內部管理；〇六九契約、類似契約或其他法律關係事務；一〇九

教育或訓練行政；一一六場所進出安全管理；一二九會計與相關服務；一三〇會議管理；一三五資(通)訊服務；一三六資(通)訊與資料庫管理；一三七資通安全與管理；一四五僱用與服務管理；一五〇輔助性與後勤支援管理；一五二廣告或商業行為管理；一五七調查、統計與研究分析；一八一其他經營合於營業登記項目或組織章程所定之業務；一八二其他諮詢與顧問服務；公務聯繫往來等運用。

3.2.2 個人資料：

本計畫所稱之個人資料，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。

3.3 個人資料之蒐集、處理與利用方式

3.3.1 依前條個人資料蒐集之特定目的及必要性，蒐集、處理及利用個人資料，並定期清查所保有之個人資料現況。

3.3.2 所屬人員為執行業務所蒐集或委託他人蒐集之個人資料，均視為公司所蒐集持有，並接受監督。

3.3.3 委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託者為適當之監督並與其明確約定相關監督事項。

3.3.4 指定之專責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個人資料，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。

3.3.5 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個人資料保護法之規定。

3.4 風險評估及管理機制

3.4.1 風險評估：

定期評估下列風險（包括但不限於）之高低，並視風險之高低，採取必要之控管措施，以降低個資遭竊取、竄改、毀損、滅失或洩漏之風險。

(1) 經由廠商電腦下載或外部網路入侵而外洩。

(2) 經由接觸書面契約書類而外洩。

(3) 員工及第三人竊取、毀損或洩漏。

(4) 業務間互為傳輸時之外洩（包括分公司間傳輸、與相關業者間傳輸等）。

3.4.2 管理機制：

(1) 藉由使用者代碼、識別密碼設定保護個人資料檔案

(2) 藉由文件妥適保管(置於上鎖櫃子或抽屜)，以保護個人資料紙本文件。

(3) 定期進行網路資通安全維護及控管。

(4) 數位資料以加密方式傳輸。

(5) 加強對員工之管制及設備之強化管理。

(6) 加強對員工個資保護意識教育訓練

3.5 事故之預防、通報及應變機制

3.5.1 預防：

同仁如因其工作執掌而須輸出、輸入個人資料時，應參照「資訊處理作業辦法」敏感與機密等級處理要點，同時在使

用範圍及使用權限內為之。

3.5.2 通報及應變：

發現個人資料遭竊取、竄改、毀損、滅失或洩漏應向公司與機關通報，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。對於個人資料遭竊取之當事人，以書面或簡訊方式通知使其知悉並說明公司已採取之處理措施。最後，針對事故發生原因研議改進措施。

3.6 資料安全管理、人員管理及設備安全管理

3.6.1 資料安全管理：

(1) 電腦存取個人資料之管控：

A. 員工應妥善保管個人電腦存取資料之硬體，並設定登入及螢幕保護程式密碼。個人資料使用完畢，應即退出電腦使用檔案，不得留置於電腦上。下班前應關閉電腦電源，並將所保有其他個人資料之媒介物置於專用抽屜內上鎖保管。

B. 員工如因其工作職掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，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。

C. 個人資料檔案使用完畢應即退出，不得任其停留於電腦畫面上。

D. 定期進行電腦系統防毒、掃毒之必要措施。

E. 重要個人資料（如病歷、醫療、基因、性生活、健康檢查、犯罪前科）應另加設管控密碼，非經陳報主管核可，

並取得密碼者，不得存取。

F. 存放個人資料電子檔案之個人電腦，不得直接作為公眾查詢之前端工具。

G. 詳應參照「資訊處理作業辦法」敏感與機密等級處理要點。

(2) 紙本資料之保管：

A. 公司保有個人資料存在於紙本者，應儲存於上鎖之保管箱或檔案室內，僅業務主管有開啟調閱權限，其他所屬人員因業務需要而須調閱或使用個人資料者，應提出申請，經業務主管人員同意後調閱或使用。員工非經廠商負責人或營業處所主管同意不得任意複製或影印。

B. 儲存個人資料紙本之保管箱或檔案室內，應設置防火裝置及防竊措施。儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。主機置放之機房應設置門禁、監視錄影及消防滅火設備。

C. 個人資料之紙本丟棄時，應先以碎紙設備進行處理。

D. 詳應參照「資訊處理作業辦法」敏感與機密等級處理要點。

3.6.2 人員管理：

(1) 依業務需求，應設定所屬員工(例如主管、非主管員工)不同之權限，以控管其個人資料之情形。

(2) 人員使用電腦設備蒐集、處理、利用個人資料，應以專屬帳號密碼登入電腦系統，存取個人資料檔案權限應與所職掌業務相符。專屬帳號密碼均應保密，不得洩漏或與他人

共用。

(3) 員工每三個月應變更識別密碼乙次，密碼長度不得低於 8 碼，且必須符合密碼複雜度原則。

(4) 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。

(5) 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）。

(6) 因業務需要而須利用非權限範圍之特定個人資料者，應事前提出申請，經業務主管人員同意後開放權限利用。

(7) 人員均應簽署保密協定，就於任職期間因業務所接觸個人資料均負保密義務。

(8) 負責個人資料檔案管理人員於職務異動時，應將保管之檔案資料移交，接辦人員應另行設定密碼。

3.6.3 設備安全管理：

(1) 建置個人資料之有關電腦設備，應定期修補作業系統、所安裝軟體安全性更新，維持最新版本，以避免有安全性漏洞遭駭客入侵竊取個資。

(2) 處理或保有個人資料之個人電腦，必須啟動 15 分鐘以內具密碼設定之螢幕保護機制，且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數位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。

(4) 保有之個人資料檔案應定期(例如：每二週)備份；當更新設備時，應注意備份資料或備份載體之安全保護措施。

(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、毀損、滅失或洩漏等事故之機制。

(6) 電腦、行動裝置或其他可攜式儲存媒體需報廢汰換或轉作其他用途時，應檢視該設備所儲存之個人資料是否確實刪除。

(7) 更新或維修電腦設備時，應指定專人在場，確保個人資料之安全及防止個人資料外洩。

3.7 認知宣導及教育訓練

3.7.1 公司每年進行個人資料保護法相關教育訓練至少一次，使員工知悉應遵守之規定。前述課程資料及簽到名冊等相關紀錄應留存備查。

3.7.2 對新進人員應於新進人員訓練課程中，宣導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，且實施課後評量，相關訓練記錄亦應留存備查。

3.8 資料安全稽核機制

3.8.1 定期(每年至少 1 次)辦理個人資料檔案安全維護稽核，查察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：

(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。

(4) 稽核情形及結果應載入稽核報告中。

3.9 使用記錄、軌跡資料及證據保存

3.9.1 公司建置含個人資料之核心業務，應啟用必要的軌跡日誌，其個人資料使用之登入、登出、查詢、變更或刪除紀錄，應建置日誌伺服器(log Server)留存。

3.9.2 個人資料紙本或電子檔案之調閱使用，應填寫「個資檔案調閱申請暨審核表」，留存調閱單位或機關、調閱者、調閱日期與時間、調閱目的、調閱單位與被調閱單位主管簽名核可等必要欄位。

3.10 個人資料安全維護之整體持續改善

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，並留存相關存取軌跡紀錄至少 5 年：

3.10.1 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

3.10.2 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。

3.10.3 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。

3.11 個人資料蒐集處理利用程序與作業辦法

3.11.1 詳參照「個人資料蒐集處理利用管理程序書」

3.11.2 詳參照「個人資料請求作業辦法」

3.11.3 詳參照「個人資料交換管理作業辦法」

4. 附件

4.1 921P03_個人資料蒐集處理利用管理程序書

4.2 921W17_個人資料請求作業辦法

4.3 921W18_個人資料交換管理作業辦法