台灣牙易通股份有限公司

資訊安全政策

機密等級:公開
文件編號:ISMS-01-01
發行日期:113年06月01日
修訂日期:113年06月01日
版次:1.1

版本記錄

版本	日期	修訂說明	備註
1.0	112年08月21日	初版	
1.1	113年06月01日	統一名詞及同步組織要求	

目 錄

1 目的

鑑於資訊安全乃維繫各項服務安全運作之基礎且包含雲端資訊安全管理如ISO 27017之雲端安全強化管理，為確保台灣牙易通股份有限公司（以下簡稱本公司）具備共識落實資訊安全的使命，特訂定資訊安全政策（以下簡稱本文件），做為本公司資訊安全管理系統的最高指導原則。

2 目標

本公司資訊安全目標為確保核心系統管理業務之機密性、完整性與可用性。並依各階層與職能定義及量測資訊安全績效之量化指標，以確認資訊安全管理系統實施狀況及是否達成資訊安全目標。

2.1 機密性（Confidentiality）：應避免本公司任何敏感資訊洩露於網際網路。

2.2 完整性（Integrity）：應確保本公司敏感資料之正確性。

2.3 可用性（Availability）：應確保本公司所持有的重要資料確實備份。

3 適用範圍

本公司。

4 組織與權責

為確保資訊安全管理系統能有效運作，應明定資訊安全組織及權責，以推動及維持各類管理、執行與查核等工作之進行。

4.1 應成立資訊安全組織統籌資訊安全事項推動。

4.2 管理階層應積極參與及支持資訊安全管理制度，提供相關資源，並分配適當權責。

4.3 適用範圍內之組織與人員皆應遵守本政策、智慧財產權及個人資料保護法。

4.4 適用範圍內之組織與人員均有責任透過適當機制，通報資訊安全事件或弱點。

5 實施原則

應依據規劃（Plan）、執行（Do）、查核（Check）及持續改善（Action）循環模式，以週而復始、循序漸進的精神，確保資訊安全之有效性及持續性。

6 審查與評估

6.1 本文件應至少每年評估審查一次，考量法令法規、科技變化、關注方期望、業務活動、內部管理與資源等最新現況，確保資訊安全實務作業之有效性。

6.2 本文件應依據審查結果進行修訂，並經資安暨個資委員主委審閱同意和發佈後始生

效。

6.3 本文件訂定或修訂後應以適當方式(例:E-Mail或網站公告)告知利害關係人，如:所屬員工、供應商、客戶、外部稽核人員等。

台灣牙易通股份有限公司

個人資料保護管理政策

發行日期:112年10月01日

最新版本以網路公告為準

1 目的

台灣牙易通股份有限公司（以下簡稱本公司）為落實個人資料之保護及管理並符合中華民國「個人資料保護法」及其施行細則之要求，參酌「資訊安全管理系統(ISO/IEC 27001)」及「隱私資訊管理系統(ISO/IEC 27701)」，確保機敏資訊、個人資料及相關系統、設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或毀損等風險，特訂定個人資料保護管理政策（以下簡稱本政策）。

2 個人資料保護管理政策

落實個資保護，降低營運風險

全體同仁貫徹執行個人資料管理制度(PIMS)，以加強規範個人資料之保障，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度，持續進行監控、審查及稽核個資保護制度的工作。

3 目標

本公司個人資料保護管理之目標如下：

3.1 依「個人資料保護法」、「個人資料保護法施行細則」與相關標準、規範要求，保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程。

3.2 為保護本公司業務相關個人資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。

3.3 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。

3.4 為提升同仁個人資料保護安全意識，每年不定期辦理個人資料保護宣導教育訓練。

3.5 每年針對個人資料作業流程進行個人資料檔案風險評估，鑑別可接受風險等級並執行風險處理。

4 個人資料之蒐集與處理

本公司因營運及執行業務所需，取得或蒐集之自然人姓名、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等，應遵循我國「個人資料保護法」（以下簡稱個資法）等法令，不過度且符合目的、相關且適當，並公平與合法地從事個人資料之蒐集與處理。且依個資法第五條規定，對於個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，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。

5 個人資料之利用及國際傳輸

5.1 本公司於利用個人資料時，除應依個資法之特定目的必要範圍內為之外，如需為特

定目的以外之利用時，將依據個資法第二十條之規定辦理；倘有需取得當事人同意之必要者，本公司應依法取得當事人之同意。

5.2 本公司所蒐集、處理之個人資料，應遵循我國個資法及本公司個資管理制度之規範，且個人資料之使用為本公司營運或業務所需，方可為本公司承辦同仁利用。

5.3 本公司取得之個人資料，如有進行國際傳輸之必要者，定謹遵不違反國家重大利益、不以迂迴方法向第三國（地區）傳輸或利用個人資料規避個資法之規定等原則辦理，又，倘國際條約或協定有特別規定、或資料接受國對於個人資料之保護未有完善之法令致有損害當事人權益之虞者，本公司將不進行國際傳輸，以維護個人資料之安全。

6 個人資料之調閱與異動

當本公司接獲個人資料調閱或異動之需求時，應依個資法及本公司所訂之程序，於合法範圍內進行當事人之個人資料查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用、請求刪除。

7 個人資料之例外利用

7.1 本公司因業務上所擁有之個人資料負有保密義務，不得對第三人揭露，除有下列情形外，應符合個資法第二十條及相關法令規定，並應以正式公文查詢：

6.1.1司法機關、監察機關或警政機關因偵查犯罪或調查證據所需者。

6.1.2其他政府機關因執行公權力並有正當理由所需者。

6.1.3與公眾生命安全有關之機關（構）為緊急救助所需者。

7.2 本公司對個人資料之利用，除個資法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。但有個資法第十九條或第二十條所列情形之一者，得為特定目的外之利用。

8 個人資料之保護

8.1 本公司已成立個人資料保護組織，明確定義相關人員之責任與義務。

8.2 本公司已建立與實施個人資料管理制度 (PIMS)，以確認本政策之實行；全體員工及委外廠商應遵循個人資料管理制度（PIMS）之規範與要求，並定期審查個人資料管理制度(PIMS)之運作。

8.3 本公司係以嚴密之措施、政策保護當事人之個人資料，包括本公司之所有教職員工生，均受有完整之個資法及隱私權保護之教育訓練。倘有洩露個資之情事者，將依法追究其民事、刑事及行政責任。

8.4 本公司之委外廠商或合作廠商與本公司業務合作時，均應簽訂保密契約，使其充分瞭解個人資料保護之重要性及洩露個資之法律責任。倘有違反保密義務之情事者，將依法追究其民事及刑事責任。

9 利害關係人之參與及期許

本公司個人資料保護及管理決議事項應納入「資安管理委員會」報告，涉及重大決議之會議紀錄應提報主管機關及利害關係人(如本公司員工及其他與本公司相關人士等)，如有任何回饋事項，將列入下次管理委員會會議之討論議題。

10 個人資料保護管理政策修訂

本公司之個人資料保護政策，每年定期或因時勢變遷或法令修訂等事由，予以適當修訂，並經本公司「資安管理委員會」通過後施行，修訂時亦同。

11 公告實施

本政策核定後，應以適當方式周知全體人員以落實執行。