版本修訂紀錄表

文件版本	制/修訂日期	修訂重點內容	修訂人員
A	2023/01/07	初稿	潘彣昕
B	2024/11/15	修改2.範圍，針對項次5.作業內容的控制項目重新編排以及加入相關文件的編號。	Judy
C	2026/02/04	依據驗證範圍進行修訂範圍	Kasen

1. 目的：

本適用性聲明之設計為適用於本公司資訊安全管理系統控制項目說明，但鑑於類型、規模、資源、業務性質等因素，若列出之任何條款無法適用單位時，可考慮予以排除，但必須在不影響單位提供資訊安全能力與責任之情況下，並提出理由。其中應包含選擇之控制目標與控制措施項目與理由，以及排除條款之內容與理由，作為執行系統與稽核時的依據。

2. 範圍：

本公司所執行之產品客製化軟體開發作業及雲端環境(GCP)維運管理。

3. 權責：

3.1. 適用性聲明的項目鑑定：資訊安全管理委員會。

3.2. 適用性聲明審查：管理代表。

3.3. 適用性聲明核准：主任委員。

4. 名詞釋義：無。

5. 作業內容：

控制項目		適用 Y/N	控制措施描述	相關文件
A.5組織控制				
A.5.1	資訊安全政策	Y	為有效執行資訊安全系統管理，本公司藉由制定資訊安全政策，以做為任職同仁與相關利害團體資訊安全遵循依據。	ISMS-1-001資訊安全政策
A.5.2	資訊安全之角色及責任	Y	本公司在推動資訊安全事務時，均透過正式的組織與管理階層授權，界定資訊安全責任。	ISMS-2-002資訊安全組織與管理審查程序
A.5.3	職務區隔	Y	針對衝突之職權加以區隔，已維持作業監控及管控。	ISMS-2-002資訊安全組織與管理審查程序
A.5.4	管理階層責任	Y	本公司藉由執行資訊安全管理系統(ISMS)過程中宣導與要求任職同仁、委外廠商以及第三方使用者遵守資訊安全政策與有關程序。	ISMS-2-002資訊安全組織與管理審查程序
A.5.5	與權責機關之聯繫	Y	本公司對於處理資訊安全事件已建立標準處理程序，包含通	ISMS-2-017資訊安全事故管理程序

			報窗口的聯繫，以確保在緊急事件發生時，能夠根據事件的情況通報適當的單位。	
A.5.6	與特殊關注群組之聯繫	Y	為取得威脅情資及相關技術漏洞訊息，應與原廠或相關協會、論壇保持聯繫	ISMS-2-013監控與防毒管理程序
A.5.7	威脅情資	Y	建立威脅情資取得、分析、通報及處置作業，以防範可能之風險。	ISMS-2-013監控與防毒管理程序
A.5.8	專案管理之資訊安全	Y	要設施設備之採購或變更專案進行時，依「資訊資產管理程序」，系統開發與維護之專案進行時，依「系統開發與維護程序」，營運流程或項目變更之專案進行時，依「營運持續管理程序」，考量專案中使用之資訊資產機密、完整、可用性之適切性，確保專案資訊安全。	ISMS-2-007資訊資產管理程序 ISMS-2-015系統開發與維護管理程序 ISMS-2-018營運持續管理程序
A.5.9	資訊及其他相關聯資產之控制措施清冊	Y	本公司為有效管理內部資訊資產，並對資訊資產清楚標示與分級，明定資產所有人及資產保管人等角色。	ISMS-2-007資訊資產管理程序
A.5.10	可接受使用資訊及其他相關聯資產	Y	本公司對於資訊資產的性質發生變動，或是新的資訊資產安裝、設置時，必須明確資產在可接受的情況下方可允許使用。	ISMS-2-007資訊資產管理程序
A.5.11	資產之歸還	Y	本公司於員工離職或職位變更時，要求有效移交並歸還資產	ISMS-2-006人力資源與訓練管理程序
A.5.12	資訊之分類分級	Y	本公司為有效管理內部資訊機密性，對資訊類資產設定標準以管理資訊標示與分級方法	ISMS-2-007資訊資產管理程序
A.5.13	資訊之標示	Y	本公司為有效管理內部資訊機密性，對資訊類資產設定標準以管理資訊標示與分級方法	ISMS-2-007資訊資產管理程序
A.5.14	資訊傳送	Y	管制傳輸媒介作業，包含各使用者權限、並制定相關資訊傳遞規範，以維護資訊交換及傳遞安全。	ISMS-2-014電子傳輸管理程序

A.5.15	存取控制	Y	本公司伺服器、資料庫之相關資訊資產建立存取控管原則，以管控存取範圍。	ISMS-2-010存取控制管理程序
A.5.16	身分管理	Y	透過申請帳號，對使用者作識別，以作為識別及維護不可否定性。	ISMS-2-010存取控制管理程序
A.5.17	鑑別資訊	Y	本公司實體範圍內的作業系統為識別網路與個人電腦的使用者，要求使用者登錄識別，並針對通行碼作強度之規範。	ISMS-2-010存取控制管理程序
A.5.18	存取權限	Y	區分不同使用者之帳號與最高管理帳號，且依照作業不同，分配不同之群組權限。	ISMS-2-010存取控制管理程序
A.5.19	供應者關係中之資訊安全	Y	委外服務交付協議中之安全管控、委外服務之定義、委外廠商之監控審查及服務變更管理。	ISMS-2-011委外資訊服務管理程序
A.5.20	於供應商協議中闡明資訊安全	Y	本公司在資訊服務委外給第三方時，於採購合約中明定與第三方服務的範圍與內容，並載明雙方之權利與義務。	ISMS-2-011委外資訊服務管理程序
A.5.21	管理ICT供應鏈中之資訊安全	Y	本公司部份資訊施備或系統因為委外進行建置或維護，故進行適當的委外資訊與通訊技術服務及產品供應鏈廠商控制機制。	ISMS-2-011委外資訊服務管理程序
A.5.22	供應商服務之監視、審查及變更管理	Y	委外廠商進行資訊設施與其有關之應用系統維護後，設備負責人會針對其服務結果進行驗收，並考量其變動所可能造成的風險，進行必要性之評估及因應。	ISMS-2-011委外資訊服務管理程序
A.5.23	使用雲端服務之資訊安全	Y	針對雲服務建立評估、監控及退出管理機制。	ISMS-2-011委外資訊服務管理程序
A.5.24	資訊安全事故管理之規劃及準備	Y	本公司根據風險評估的結果，針對相關人員的權責給予適當的界定，在發生資訊安全事件時，問題得到迅速的解決方案。	ISMS-2-017資訊安全事故管理程序

A.5.25	資訊之評鑑及決策	Y	本公司針對相關人員的權責給予適當的界定，在發生資訊安全事件時，問題得到迅速的解決方案。	ISMS-2-017資訊安全事故管理程序
A.5.26	對資訊安全事故之回應	Y	本公司針對相關人員的權責給予適當的界定，在發生資訊安全事件時，問題得到迅速的解決方案。	ISMS-2-017資訊安全事故管理程序
A.5.27	由資訊安全事故中學習	Y	本公司在資訊安全事件發生後，記錄資訊安全事件發生的過程，並且視資訊安全事件的影響程度進行定期與不定期的檢討會議，討論可能的改善機會，並且運用適當的手法進行改善、矯正措施或預防措施。	ISMS-2-017資訊安全事故管理程序
A.5.28	證據之蒐集	Y	在涉及法律行動(民事或刑事)的資訊安全事故，應收集、保存及呈現證據。	ISMS-2-017資訊安全事故管理程序
A.5.29	中斷期間之資訊安全	Y	於相關系統及服務中斷時，考量衍生可能之安全風險，並加以控制。	ISMS-2-018營運持續管理程序
A.5.30	營運持續之ICT備妥性	Y	為達營運持續性目標，應進行災害及系統中斷影響分析，識別營運中斷之關鍵因素及其影響，確保關鍵營運業務得以即時恢復。	ISMS-2-018營運持續管理程序
A.5.31	法律、法令、法規或契約要求 事項	Y	本公司收集與資安相關之法令並對其適用性進行評估，確認其適用範圍和具體適用條例，並每年針對法規有效性重新評估，以保持適用法律、法規之最新版本。	ISMS-2-019資訊安全法規鑑別
A.5.32	智慧財產權	Y	建立機制，確保本公司軟體安裝合法性	ISMS-2-019資訊安全法規鑑別
A.5.33	紀錄之保護	Y	本公司按相關法律法規要求，訂定重要紀錄之保存期限，並提供適當之保護措施。	ISMS-2-019資訊安全法規鑑別
A.5.34	隱私及PII保護	Y	本公司嚴格執行國家有關個人資料保護之相關法律法規，要求全體同仁對於客戶資料進行	ISMS-2-019資訊安全法規鑑別

			妥善管理與保護，以防止遺失或洩露個人資料之風險。	
A.5.35	資訊安全之獨立審查	Y	週期性的對資訊安全管理系統進行審查及確認，資訊安全的控制目標、控制措施、政策、過程及程序的作法	ISMS-2-002資訊安全組織與管理審查程序
A.5.36	資訊安全政策、規則及標準之 遵循性	Y	針對資訊安全管理系統進行內部稽核，每次稽核範圍應涵蓋與資訊安全管理系統相關之所有單位，確保職責範圍內之所有資訊安全程序及流程正確無誤，且符合資訊安全政策與標準。	ISMS-2-003資訊安全稽核管理程序
A.5.37	書面記錄之運作程序	Y	本公司依資訊安全管理要求，建立相關程序文件，並加強文件管理。	ISMS-2-001資訊安全文件與記錄管理程序
A.6人員控制				
A.6.1	篩選	Y	於聘僱之前，明訂員工、訂約人和第三者之安全與角色之責任。 於人員增補需求，詳細說明增補人員之職責及應具備之條件。	ISMS-2-006人力資源與訓練管理程序
A.6.2	聘用條款及條件	Y	本公司均要求同仁及廠商在詳細閱讀並簽署保密承諾書。	ISMS-2-006人力資源與訓練管理程序
A.6.3	資訊安全認知及教育訓練	Y	本公司員工應建立資訊安全觀念並確實遵守資訊安全相關管理規章及制度，且不定期舉辦資訊安全教育訓練。	ISMS-2-006人力資源與訓練管理程序
A.6.4	懲處過程	Y	本公司為配合資訊安全系統運作，對於違反資訊安全政策與程序之人員，給予懲處。	ISMS-3-001員工獎懲辦法
A.6.5	聘僱終止或變更後之責任	Y	本公司於員工離職或職位變更時，要求有效移交並歸還資產。	ISMS-2-006人力資源與訓練管理程序
A.6.6	機密性或保密協議	Y	本公司均要求同仁及廠商在詳細閱讀並簽署保密承諾書。	ISMS-2-006人力資源與訓練管理程序
A.6.7	遠距工作	Y	本公司作業可依需求，透過遠距工作進行，並針對遠距工作之開放進行控制。	ISMS-2-010存取控制管理程序

A.6.8	資訊安全事件通報	Y	建立通報系統，分類資訊安全事件的等級，在資訊安全事件發生時，通報適當的層級。	ISMS-2-017資訊安全事故管理程序
A.7實體控制				
A.7.1	實體安全周界	Y	明確劃分安全區域範圍，並且書面化實體範圍界定結果。訪客、廠商進出需登記，且要求由相關承辦人員陪同，以達實體環境之安全控管。	ISMS-2-008實體安全管理程序
A.7.2	實體進入	Y	設定資訊安全區域使用門禁、保全、等方式進行監控。	ISMS-2-008實體安全管理程序
A.7.3	保全之辦公室、房間及設施	Y	設定資訊安全區域使用門禁、保全、等方式進行監控。	ISMS-2-008實體安全管理程序
A.7.4	實體安全監視	Y	針對安全區域執行監控作業，以防範未經授權之進入。	ISMS-2-008實體安全管理程序
A.7.5	防範實體及環境威脅	Y	本公司管制區域內建置時考慮了火災、水災、地震、雷電、人員傷亡、竊盜、破壞等等列入威脅中，並且進一步的結合弱點考慮資訊安全系統的風險與適當的處置措施。	ISMS-2-008實體安全管理程序
A.7.6	於安全區域內工作	Y	本公司規劃安全區域，並使用門禁、保全等方式進行監控。	ISMS-2-008實體安全管理程序
A.7.7	桌面淨空及螢幕淨空	Y	以螢幕保護及資訊分級管制作業，確保桌面及螢幕資訊之安全管理。	ISMS-2-010存取控制管理程序
A.7.8	設備安置及保護	Y	本公司重要的資訊設備，一律設置安全存放區，並施予保養與維護。	ISMS-2-008實體安全管理程序
A.7.9	場所外資產之安全	Y	資訊設備放置於公司外部時，依其安全要求配置其管控措施。	ISMS-2-008實體安全管理程序
A.7.10	儲存媒體	Y	針對儲存式媒體使用進行管控，防止可能之惡意程式威脅或機密資料外洩威脅。	ISMS-2-007資訊資產管理程序 ISMS-2-009行動裝置管理程序
A.7.11	支援之公用服務事業	Y	本公司管制區域內設立不斷電系統以維持正常供電，並對電、纜線路進行維護。	ISMS-2-008實體安全管理程序

A.7.12	佈纜安全	Y	本公司管制區域內對電、纜線路進行設置管理及標示。	ISMS-2-008實體安全管理程序
A.7.13	設備維護	Y	本公司對管制區域內內的資訊設備及系統等維護採取自維以及委外的方式並行；在設備異常時，依據標準程序進行處理。	ISMS-2-008實體安全管理程序
A.7.14	設備汰除或再使用之保全	Y	本公司資訊設備之調配、處理及再利用均應符合安全使用的原則，並將資料移除。	ISMS-2-007資訊資產管理程序
A8技術控制				
A.8.1	使用者端點裝置	Y	針對使用者之資訊設備，建立使用規則及管控機制，確保資訊安全得到全面性管理。	ISMS-2-007資訊資產管理程序 ISMS-2-009行動裝置管理程序
A.8.2	特殊存取權限	Y	管理者帳號需提出申請，並控制其目的、範圍及需使用特權之期間。	ISMS-2-010存取控制管理程序
A.8.3	資訊存取限制	Y	本公司對於資訊系統存取，制定程序，以管控存取範圍。	ISMS-2-010存取控制管理程序
A.8.4	對原始碼之存取	Y	原始碼應加以保存，並按其版次狀況予以識別管理，並針對原始碼之存取設定權限管理。	ISMS-2-015系統開發與維護管理程序
A.8.5	安全鑑別	Y	本公司所屬資訊系統皆需經過適當的使用者登錄介面才可進入操作系統。	ISMS-2-010存取控制管理程序
A.8.6	容量管理	Y	本公司資訊系統藉由監控軟硬體使用狀況及未來需求預測，做為系統容量與使用效能的規劃	ISMS-2-013監控與防毒管理程序
A.8.7	防範惡意軟體	Y	本公司負責提供符合需求的防毒軟體等技術工具，對技術工具進行升級及更新並透過資安宣導，加強電腦終端用戶對惡意程式之控制責任。	ISMS-2-013監控與防毒管理程序
A.8.8	技術脆弱性管理	Y	為防止資訊技術弱點造成重大資安事故發生，執行弱點識別與因應作業。	ISMS-2-013監控與防毒管理程序

A.8.9	組態管理	Y	針對重要系統及設備進行配置管理，包含版本控制、漏洞修補及安全設定。	ISMS-2-007資訊資產管理程序
A.8.10	資訊刪除	Y	針對資料建立保存及刪除管理機制，以避免機密資訊外流之風險。	ISMS-2-007資訊資產管理程序
A.8.11	資料遮蔽	Y	針對資料，依其機密等級、存取必要性，進行資料加密、去識別、隱藏或遮罩等機制，以避免機密資訊外流之風險。	ISMS-2-007資訊資產管理程序
A.8.12	資料洩露預防	Y	針對資料傳輸、網路安全、資產管理及存取權限進行管制，以避免機密資訊外流之風險。	ISMS-2-007資訊資產管理程序
A.8.13	資訊備份	Y	本公司定期實施備份作業，以確保在發生系統錯誤時能順利復原。	ISMS-2-012資料備份管理程序
A.8.14	資訊處理設施之多備	Y	以營運重要性考量，建立必要之備援系統，以確保資訊資產對營運持續之可用性及完整性。	ISMS-2-018營運持續管理程序
A.8.15	存錄	Y	透過資訊設備的系統事件記錄，以紀錄、保存、分析與進一步的改善行動，並作為分析資訊安全事件之資料來源。	ISMS-2-013監控與防毒管理程序
A.8.16	監視活動	Y	管理者及操作者作業透過系統事件記錄，以紀錄、保存、分析。	ISMS-2-013監控與防毒管理程序
A.8.17	鐘訊同步	Y	定期校正系統作業時間，維持系統稽核紀錄的正確性及可信度，最為事後法律上或是紀律處理上的重要依據。	ISMS-2-013監控與防毒管理程序
A.8.18	具特殊權限公用程式之使用	Y	針對資訊系統特殊權限公用程式管制其使用權限及範圍。	ISMS-2-010存取控制管理程序
A.8.19	對運作中系統之軟體安裝	Y	為確保資訊系統之穩定性，相關軟體之安裝、設定及維護須由系統負責人執行。	ISMS-2-010存取控制管理程序
A.8.20	網路安全	Y	本公司規範網路使用規則，明訂網路用途以及不可為之事項。	ISMS-2-020網路安全管理程序

A.8.21	網路服務之安全	Y	網路使用防火牆政策控制等方法，來進行網路服務安全的管控。	ISMS-2-020網路安全管理程序
A.8.22	網路區隔	Y	藉由防火牆管制，以降低受外部網路攻擊或入侵之風險。	ISMS-2-020網路安全管理程序
A.8.23	網頁過濾	Y	管理對外部網站的連線，以減少暴露於惡意內容	ISMS-2-020網路安全管理程序
A.8.24	密碼技術之使用	Y	置於公開網路應用服務採取適當之加密機制(如Https)，以確保資料傳遞之安全性。	ISMS-2-020網路安全管理程序
A.8.25	安全開發生命週期	Y	建立軟體及系統開發之規則，並應用至公司之系統開發。	ISMS-2-015系統開發與維護管理程序
A.8.26	應用系統安全要求事項	Y	針對應用系統開發時，評估及建立安全規格及要求，以作為後續執行之依據。	ISMS-2-015系統開發與維護管理程序
A.8.27	安全系統架構及工程原則	Y	確保新系統開發或更新系統時，規範系統安全規格與功能分析。	ISMS-2-015系統開發與維護管理程序
A.8.28	安全程式設計	Y	建立系統開發安全編碼規則，以維持應用系統安全基準。	ISMS-2-015系統開發與維護管理程序
A.8.29	開發及驗收之安全測試	Y	依照系統規格要求進行系統安全要求之驗收測試。	ISMS-2-015系統開發與維護管理程序
A.8.30	委外開發	Y	針對委外開發作業，確認其開發作業符合公司安全政策要求	ISMS-2-015系統開發與維護管理程序
A.8.31	開發、測試及運作環境之區隔	Y	本公司資訊系統進行開發過程，要求安裝至正式的系統運行前，必須要有安全的測試環境與模擬數據以供給系統測試	ISMS-2-015系統開發與維護管理程序
A.8.32	變更管理	Y	本公司資訊設備與系統在變更時，必須進行風險識別，並加以控制。	ISMS-2-007資訊資產管理程序
A.8.33	測試資訊	Y	系統開發測試資料採虛擬資料、去識別化資料，進行作業，如使用真實資料，進行完善管理作業。	ISMS-2-015系統開發與維護管理程序
A.8.34	稽核測試期間資訊系統之保護	Y	系統管理者使用稽核技術工具進行控管時，如防毒或弱掃，應利用離峰時間進行作業，以對營運之影響降至最低。	ISMS-2-013監控與防毒管理程序

6.相關文件：無。

7.使用表單：無。