中美聯合實業股份有限公司

資通安全政策及作業程序

一、資通安全政策

目的

為確保公司所屬之資訊資產的機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，並衡酌本公司之業務需求，訂定本政策。

適用範圍

資訊安全管理涵蓋以下管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來各種可能之風險及危害。管理事項如下：

1. 資訊安全政策(訂定與評估)。
2. 資訊安全組織。
3. 人力資源安全。
4. 資產管理。
5. 存取控制。
6. 密碼(加密控制)。
7. 實體與環境安全。
8. 運作安全。
9. 通訊安全。
10. 資訊系統取得、開發及維護。
11. 供應者關係。
12. 資訊安全事故管理。
13. 營運持續管理之資訊安全層面。
14. 遵循性。

本公司之內部人員、委外服務廠商與訪客皆應遵守本政策。

為維護本公司資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全，以達成下列目標：

1. 保護本公司核心系統業務活動資訊，避免未經授權的存取，確保其機密性。
2. 保護本公司核心系統業務活動資訊，避免未經授權的修改，確保其正確性與完整性。
3. 建立資訊業務永續運作計畫，確保本公司核心系統業務活動之持續運作。
4. 本公司核心系統之業務活動執行須符合相關法令或法規之要求。

責任

- 1.本公司應成立資訊安全單位籌資訊安全事項推動。
- 2.管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序以實施本政策。
- 3.所有人員和委外服務廠商均須依照相關安全管理程序以維護資訊安全政策。
- 4.所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
- 5.任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司之相關規定進行議處。

管理指標

為評量資訊安全管理目標達成情形，本公司特訂定資訊安全管理指標如下：

- 1.因人為或作業疏失及未經授權的存取之資安事故，每年不得超過二件。
- 2.確保本公司機房維運服務達全年上班時間98%(含)以上之可用性。
- 3.確保滿足各關鍵業務系統之服務可用率達全年上班時間之99%以上。
- 4.為確保本公司資訊安全措施或規範符合現行法令、法規之要求，每年至少需執行內部稽核乙次。
- 5.應適當保護本公司資訊資產之機密性與完整性，每年至少需進行資訊資產盤點及風險評估乙次。

定性化指標

- 1.定期審查本公司資訊安全組織人員執掌，以確保資訊安全工作之推展。
- 2.應符合主管機關之要求，依員工職務及責任提供適當之資訊安全相關訓練。
- 3.應加強本公司資訊機房設施之環境安全，採取適當之保護及權限控管機制。
- 4.應加強存取控制，防止未經授權之不當存取，以確保本公司資訊資產資訊安全政策

受適當的保護

- 1.確保資訊不會在傳遞過程中，或因無意間的行為透露給未經授權的第三者。
- 2.確保所有資訊安全意外事故或可疑之安全弱點，都應依循適當之通報機制向上反應，並予以適當調查及處理。

本政策應隨時反映政府法令、技術及業務等最新發展現況，以確保本公司永續運作及提供商務經營網路服務之能力。

二、資通安全作業程序

第一章 總則

- 一、本程序依本公司資通安全政策訂定之。
- 二、本公司各單位經核示後得依本要點另訂定作業程序。
- 三、本公司資通安全推動組織如下：

本公司資安小組(資訊處)推動本公司資通安全管理事宜。

四、本要點用詞，定義如下：

- (一) 電腦機房：包含資訊機房、通訊機房、監控室、媒體儲存區及附屬機電室。
- (二) 電腦系統：包含本公司提供之個人電腦及手攜式裝備、網路設備、伺服器、資料儲存設備、附設或嵌入於儀器之電腦設備等，及其作業系統與應用系統。
- (三) 敏感性電子資料：係指公司機密，以及涉及依規定應限制公開或不予提供者。

第二章 人員管理暨資通安全訓練

五、本公司人員應注意下列資通安全事項：

- (一) 依相關法規負保守公司機密之義務。
 - (二) 職務為可接觸機密性或敏感性資料者，應於任務指派前閱讀相關保密條款，並簽名以示認知該職務之資通安全規定。
 - (三) 重要應用系統之發展、維護、管理及操作之人員，應妥適分工，分散權責，並視需要建立管控機制，實施人員輪調，建立人力備援制度。
 - (四) 各級主管應督導所屬人員妥為辦理資通作業，以確保資通安全，防範不法及不當行為。
 - (五) 資通作業人員於離職或職務調動時應辦理資通資產交接或歸還，並應立即辦理權限異動或帳號移除。
- 六、本公司應定期舉辦資通安全相關之教育訓練，促使同仁瞭解資通安全之重要性及各種可能的資通安全風險，以提高同仁資通安全意識，促其確實遵守資通安全規定。

七、本公司人員應依內控辦法規定，依其職務性質完成相關之資通安全訓練。

八、委外作業資通安全管理事項：

- (一) 本程序所稱委外作業，係指委託廠商辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務）；委託單位即指委託廠商辦理上揭受託業務之單位。
- (二) 本公司應監督受託業務之資通安全維護情形。
- (三) 委外契約應載明下列事項：
 - 1. 廠商應遵循之資通安全、保密條款及作業相關之法規要求。
 - 2. 各項資通安全控管要求，以明確告知委外廠商應遵循事項。
 - 3. 相關資通資產之機密性、完整性、可用性及法規性要求。
 - 4. 本公司有對委外廠商進行資通安全稽核之權利。
- (四) 本公司應於簽約後，提供委外廠商資通安全相關作業方式及規定。
- (五) 委外廠商及其相關人員於契約期間出入本公司時，須佩戴識別證，以供人員安全控管及掌握。
- (六) 委外廠商及其相關人員於非上班時間作業時(緊急情況)，應事先取得本公司同

意，且本公司應派員陪同。

(七)委外廠商駐點服務人員、實際參與履行契約人員及經常至本公司各單位資訊部門洽公之業務人員，均應簽署保密切結書。

第三章 電腦機房安全管理

九、電腦機房(以下簡稱機房)之規劃、設計與建置應依下列原則辦理：

- (一) 考量安全與最大之電力容量、空調散熱能力及地板承重。
- (二) 室內建材須耐燃且符合國家標準。
- (三) 供電設備如變壓器、不斷電系統、電池組等須有安全保護措施。
- (四) 裝設無腐蝕性自動滅火設備。
- (五) 裝設環境監測或監控設備。

另考量實際可行性，宜參考以下原則辦理：

- (一) 機電室與機房其他部分間保留安全距離，並各自具獨立之空氣及水循環系統。
- (二) 裝設監控空調水位、主電源斷電等之警示設備。
- (三) 考慮不同冷却方式之備援空調設備。

十、機房內所裝置之電腦系統及相關設備，不應超出安全電力容量、空調散熱能力及地板承重；並嚴禁超載使用。

十一、機房內電腦機櫃、單獨系統及相關設備之間，應保留作業及散熱所需之足夠空間。

十二、機房應有門禁管制，防止未經授權者進出；機房進出管制應依下列原則辦理：

- (一) 人員進出機房均須登記，非機房管理人員未經許可不得進入機房。
- (二) 廠商維護人員進入機房，應由機房管理人員全程陪同。
- (三) 不得攜帶非工作所需物品進入機房。
- (四) 機房設備送修或修妥送回，均須登記。

十三、機房之日常作業應依下列原則辦理：

- (一) 機房定期執行清潔作業。
- (二) 機房設施定期保養，定期辦理安全防護演練。
- (三) 機房內廢棄物儘速移除。

十四、機房值班人員應辦理下列事項：

- (一) 機房門禁及進出管制。
- (二) 機房重要設備與設施之監控，異常狀況之通報、聯繫及因應。
- (三) 機房內、外電腦相關設備與設施之巡察。
- (四) 機房實體環境安全之維護。
- (五) 其他交辦之機房管理事項。

十五、機房各電腦系統及重要設備應指派專責人員，辦理下列事項：

- (一) 定期監控系統或設備，確保正常運作。

- (二) 系統或設備發生異常狀況時，應即到場、透過安全連線或通訊指導值班人員等方式予以處理；必要時通知維護廠商依約處理。
異常狀況及其處理情形應即登載於機房工作日誌。
- (三) 其他交辦之系統或設備管理事項。

第四章 電腦系統安全管理

十六、電腦系統應與標準時鐘同步或定期對時，以確保系統時間之一致性。

十七、安裝作業系統應依下列原則辦理：

- (一) 作業系統應僅安裝系統運作所需之套件，各套件應僅啟用所需之服務。
- (二) 作業系統修補，如需連接網路以安裝系統修正檔時應先評估其風險。
- (三) 作業系統安裝完成後，應即完整備份。

十八、安裝於電腦系統之程式，未能確認其功能與安全性者應先行測試，測試作業應依下列原則辦理：

- (一) 不得於系統正式作業環境進行測試，測試電腦之網段應與正式作業網段適度區隔。
- (二) 如委由廠商進行測試，應嚴格規定其範圍、權限及程序；並責成廠商提供測試報告，必要時要求廠商先行提交測試計畫。

十九、電腦系統上線時應建立組態資訊，包含軟硬體版本、型號、系統啟用服務及相關參數設定等，並持續維護。

二十、對運作中之電腦系統進行異動，包含系統升級、變更設定、安裝安全性修補程式及組態變更等，應依下列原則辦理：

- (一) 異動前應先評估所需資源，包括軟硬體容量、效能、人員、時程及廠商支援等。
- (二) 應評估對相關電腦系統、應用程式之相容性及對整體資通作業環境之影響，確保異動之內容符合需求，需要時得要求相關系統管理人員協助評估。
- (三) 組態設定檔於變更前及變更後，均應匯出備份，並至少維持最近3個版本。
- (四) 異動過程中應詳細記錄所遭遇之問題及解決方法。
- (五) 異動前應進行備份及回復準備，避免無法復原造成電腦系統不可預期之損害。

二十一、各電腦系統應監控其硬體資源使用、作業系統、資料庫管理系統及網路服務等。

第五章 應用系統發展及維護安全管理

二十二、本章規定適用於本公司自行或委外開發建置、維護之應用系統。

二十三、應用系統發展或維護前，應先評估其資通安全風險，包括對相關電腦系統之安全衝擊。

二十四、應用系統開發與維護之安全管理應涵蓋下列事項：

- (一) 訂定安全運作環境，並嚴謹管理與設定，只釋出必要之最小存取權限。
- (二) 訂定網路接取安全措施。
- (三) 建立有效防止人為疏失、杜絕惡意入侵之安全控管機制。
- (四) 具備完整伺服器端安全控管。
- (五) 檢測安全弱點及漏洞，包括自行檢測及非發展者之檢測。
- (六) 規範及限制廠商可存取之系統與資料範圍。

二十五、發展應用系統，應於規劃階段，即將下列資通安全需求納入考量：

- (一) 管理者與使用者之權責。
- (二) 使用者身分認證方法。
- (三) 對系統及資料之存取控制。
- (四) 所有資料項之屬性。
- (五) 機密性及敏感性資料保護機制。
- (六) 資料備份及系統故障後回復作業需求。
- (七) 重要作業之系統紀錄。
- (八) 其他需考量之資通安全控制措施。

前項安全需求應儘量轉化為系統功能，自動執行，其餘部分由人工控管，並訂定人工安全控管規範。

二十六、應用系統之測試資料不應含有個人真實訊息、機密性或敏感性內容；若需使用真實資料進行測試時，應採行下列保護措施：

- (一) 參與測試者對資料負保護及保密之責，非因測試需要，不得閱讀內容。
- (二) 適用實際作業之存取控制措施，亦適用於測試作業。
- (三) 測試完畢後，真實資料立即刪除。

二十七、應用系統於上線執行或版本異動前應先進行測試，測試作業應依下列原則辦理：

- (一) 不得於系統正式作業環境進行測試。
- (二) 如委由廠商進行測試，應嚴格規定其範圍、權限及程序；並責成廠商提供測試報告，必要時要求廠商先行提交測試計畫。

二十八、應用系統版本異動前應進行備份及回復準備，避免無法復原造成不可預期之損害，異動過程中應詳細記錄所遭遇之問題及解決方法。

二十九、基於委外開發之實際作業需要，得核發暫時之系統辨識及通行碼供廠商使用，使用完畢後應立即取消其使用權限。

第六章 應用系統存取控制管理

三十、本公司應用系統帳號、通行碼、使用權限及存取紀錄等，應依本章規定進行管理。

三十一、帳號新增及異動管理應依下列原則辦理：

- (一) 帳號新增及異動須經申請，並經權責人員核可後，交由系統管理單位辦理，並保留紀錄。

- (二)帳號、通行碼之通知過程應有保護措施，防止被窺視竊取。
- (三)單一使用者於單一系統上僅能申請及持有單一個人帳號，因業務或特殊原因需使用兩個以上帳號，應提出申請。
- (四)帳號持有人個人資料如有變更時，應依規定更新；人員職務異動、留職停薪或離職時應依規定辦理帳號移交或註銷，未依規定辦理者，系統管理人員得逕行停止該帳號之使用。
- (五)不得共用帳號，以區分安全責任；但職務帳號得與職務代理人共同管理。

三十二、帳號持有人應遵守下列原則：

- (一)尊重他人隱私與使用權。
- (二)不得擅自使用他人帳號或修改他人檔案、資料或通行碼，亦不得置放或散布侵擾其他使用者之程式。
- (三)不得侵入未經授權使用之電腦系統。
- (四)不得傳送或散布具恐嚇性、暴力性或猥褻性之資料，或謾罵、侮辱他人等不當言論。
- (五)不得散布病毒、蠕蟲、木馬、後門等有害程式。
- (六)遵守智慧財產權有關規定，不得重製或散布侵害他人著作權之檔案。
- (七)不得寄送垃圾或廣告郵件。
- (八)不得有其他重大違規行為。

帳號持有人如有違反前項使用原則情事，系統管理人員視情節得為通知改善、縮減使用權限、停止使用或其他必要之處置。

三十三、應用系統登入管理應依下列原則辦理：

- (一)宜設定可開放連線之時間或連線逾時自動登出之機制。
- (二)除帳號、通行碼外，應依業務需求考量是否採用其他適切之身分鑑別技術。
- (三)登入作業完成後，宜顯示前一次登入成功或失敗之時間或相關訊息。
- (四)限制連續登入失敗次數之上限，登入失敗次數達上限者，應暫停該帳號一定時間之登入，或鎖定該帳號直到系統管理人員重新啟動。
- (五)必要時限定使用者之IP位址。

三十四、使用者應選擇高安全性通行碼，力求降低被破解之風險，並應妥善保管避免他人知悉。通行碼應定期更新；重要應用系統之通行碼更新週期應低於6個月。

三十五、應用系統使用存取權限管理應依下列原則辦理：

- (一)使用者權限之申請，應由權責單位依使用者執行職務之需求，以工作所需最小權限之原則核可後，交由系統管理人員執行相關設定。
- (二)未經核可之申請，系統管理人員不得進行授權作業設定。
- (三)系統管理人員進行遠端維護時，應限制其經由本公司核可之遠端連線來源。

三十六、重要應用系統應啟動系統紀錄功能，系統管理人員應保存系統紀錄檔並定期備份。

各系統應視其重要性及支援程度將下列事件列入紀錄：

- (一)系統管理人員及具備特殊權限帳號者之登入成功及失敗事件。

- (二)使用者帳號異動及對通行碼檔案之讀取與變更。
- (三)程式原始碼及執行碼之變更。
- (四)直接進入資料庫管理系統變更資料。
- (五)系統設定檔之存取及變更。

三十七、系統管理人員應依下列原則辦理存取控管作業查核：

- (一)定期辦理帳號清查，若發現帳號不當使用或持有人不再符合申請資格，系統管理人員得停止或註銷該帳號。
- (二)監控有無違反系統存取規定之安全事件，並定期檢視紀錄，分析其異常狀況。
- (三)存取紀錄檔須另行查核。
- (四)已註銷帳號之所屬檔案，得保存一定期限，原帳號持有人得於保存期限內申請重製。但儲存重製檔案之媒體應由申請者自備。

三十八、各單位開放外界連線作業之應用系統，應避免人員直接存取應用系統之資料檔，必要時得視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、代理伺服器、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統遭入侵、破壞、竄改、刪除或未經授權之存取，並記錄完整系統使用資料。

第七章 網路安全管理

三十九、本公司為維護資通安全或避免非法行為，各單位得依網路服務性質分別規範網路存取、網路服務功能或通訊協定之使用方式。

四十、各單位以固定或動態方式提供使用之IP位址，應保存其使用紀錄以備資通安全事件稽核之需。

四十一、各單位應管理網路系統及相關設備，以維持基礎網路服務系統正常運作。

四十二、各單位網路系統及設備之管理應依權責配發管理帳號並設定適當權限；除因系統限制外，不得多人共享帳號。

四十三、各單位應妥適安全控管對外連接網路之線路與設備，必要時得設防火牆或其他安全設施，以控管外界與本公司網路之資料傳輸及資源存取。

四十四、各單位利用公眾網路傳送資訊或進行交易處理，應遵守本公司相關規定；並應評估可能之安全風險，確定資料傳輸符合完整性、機密性、身分鑑別及不可否認性等安全需求。

四十五、網路之管理

本公司網路之路由接續、IP位址區段之分配管制及領域名稱登錄等管理事項由本公司資訊處負責。

本公司網路增值服務之協調與整合由資訊處負責。其有關網路之管理事項如下：

- (一) 應辦理安全維護事項，防止個人資料遭竊取、竄改、毀損、滅失或洩漏。
- (二) 為維護網路安全及效能，應區隔及調節網路流量。
- (三) 配合本公司處理網路事宜，提供相關資訊。

四十六、禁止濫用網路系統

使用者不得從事下列行為：

- (一) 盜用、冒用他人帳號或無故將個人帳號借予他人使用。
- (二) 散布電腦病毒、傳送廣告信或無用訊息或其他違反法令之行為。
- (三) 以任何方式偷窺、竊取、更改或破壞他人資訊。
- (四) 傳送或散布恐嚇、猥褻或違背善良風俗習慣之資料，或謾罵、侮辱他人等不當言論。
- (五) 濫用網路資源，影響系統正常運作或危害網路穩定之行為。

四十七、尊重智慧財產權

使用者應尊重智慧財產權，避免下列可能涉及侵害智慧財產權之行為：

- (一) 使用未經授權之電腦程式。
- (二) 下載或重製未經授權之著作。
- (三) 未經著作權人之同意，重製或散布其著作於公開之網站上。
- (四) 任意轉載作者明示禁止轉載之網路文章。
- (五) 架設網站供公眾下載未經授權之著作。
- (六) 其他可能涉及侵害智慧財產權之行為。

四十八、網路隱私權之保護

網路管理者及使用者應尊重網路隱私權，不得任意窺視個人隱私資料或有其他侵犯隱私權之行為。

四十九、違反之處置

使用者違規使用網路，本公司得視情節依公司規定懲處。違規使用網路情形嚴重者，立即停止網路使用權限。

使用者違規使用網路，其行為違法時，行為人應依民法、刑法、著作權法或其他相關法令自負法律責任。

五十、申訴機制

如違規使用網路之行為人對本公司依前點所為處置有異議時，得向本公司資訊處申訴。

第八章 電子資料安全管理

五十一、下列電子資料應依本章規定進行管理：

- (一) 供公務使用之資料庫、資料檔、文件檔及E-MAIL檔。
- (二) 電腦系統中帳號之個人資料、存取與服務紀錄。

五十二、電子資料之經管單位，包括主要管理單位資訊處及各單位使用者。

五十三、敏感性電子資料使用及存取，應遵守相關法令或規定。

其他機關非經法定程序要求本公司提供敏感性電子資料者，應予拒絕。

五十四、電子資料之存取，應設控制措施，以防止未經授權之竄改或竊取。

敏感性電子資料之存取，應採取較一般帳號通行碼機制更為嚴格之控制措施，並應注意其相關安全事項。

存有敏感性電子資料之個人電腦，應設具相當安全程度之開機通行碼。

五十五、電子資料應有備份，其儲存裝置得有備援措施。

敏感性電子資料應加密儲存；其未經加密者，不得經由公眾網路傳送或儲存於可攜式儲存媒體。

進行電子資料交換時，若需啟用新服務，應先評估其風險。

五十六、各單位使用網際網路及全球資訊網公布及流通資訊，敏感性及未經當事人同意之個人資料及文件，不得上網公布。

五十七、本公司電腦系統存有單位或個人之敏感性電子資料者，應加強安全保護措施，防止該資料遭違法或不當之竊取使用。

五十八、電腦送修，應先拔除硬碟或抹除敏感性電子資料；報廢時，應抹除或銷毀儲存之所有檔案。

可攜式儲存媒體送修或報廢時亦同。

五十九、委託其他機構或廠商蒐集、處理或利用敏感性電子資料時，應於委外契約書載明資通安全控管要求、保密條款、損害賠償等事項。

第九章 資通安全事件通報、應變及演練

六十、資訊處為本公司資通安全事件通報總窗口，依資安法及其子法相關規定，負責下列資通安全事件通報與處理事項：

(一) 本公司資通安全事件分級確認。

(二) 依相關規定通報本公司資通安全事件。

(三) 規劃資通安全事件處理程序，包括調查事件原因、確認其影響範圍並評估損失及執行緊急應變措施。

(四) 協助各單位處理資通安全事件。

(五) 資安事件通報及應變事項之定期演練。

各單位窗口負責下列資通安全事件通報與處理事項：

(一) 單位內資通安全事件初步分級。

(二) 單位資安事件依本公司管道通報資訊處總窗口。

(三) 規劃單位內資通安全事件處理程序，包括調查事件原因、確認其影響範圍並評估損失及執行緊急應變措施。

(四) 資安事件通報及應變事項之定期演練。

六十一、本公司通報程序如下：

(一) 各單位知悉資通安全事件時，立即將事件通報資訊處總窗口。

(二) 總窗口接獲資通安全事件通報後，應彙整相關事件並依相關規定確認分級及進行資安事件通報，同時依本公司管道通報受影響單位及機關。

六十二、本公司應變程序如下：

(一) 事件發生前之防護措施規劃

各單位應評估本公司資通安全事件預防需求，建置並維護適當設備及相關技術，以加強防範發生資通安全事件之能力。

(二) 損害控制機制

1. 資通安全事件發現並通報後，資訊處應依資安法及其子法規定時程復原或完成損害控制。

- 2.發生資通安全事件時，應即啟動本公司資通安全事件處理小組，進行危機處理與緊急應變措施。資安小組由資訊處主管擔任召集人，其成員由召集人指定之。
- 3.資通安全事件之原因、影響範圍、損失情況、分類、分級及應變措施等應詳加記錄，作為改善資通安全缺失、因應未來類似事件及修訂各類資通安全事件處理程序之參考。

第十章 資通安全內部稽核

- 六十三、稽核室依公司相關規定或視實際需要，經核示後資通安全內部稽核作業。
- 六十四、實施資通安全內部稽核前，稽核室應依資安及個資相關規定擬定資通安全稽核計畫書以及資通安全稽核檢查表，核示後執行。
- 六十五、資通安全稽核計畫書應至少包括：實施對象、實施時程、實施範圍、人員配置、相關規範、要點或程序。
- 六十六、實施資通安全內部稽核時，應就查核情形詳予記錄，並對所獲悉之機密性或敏感性資料負保密責任；受稽核對象應指派專人配合實施。
- 六十七、實施資通安全內部稽核後，須盡速完成以下事項：
 - (一)稽核室撰寫資通安全稽核報告，並送各受稽核對象確認。
 - (二)各受稽核對象應就資通安全稽核報告中所列缺失事項提具矯正措施或改善計畫；資安內稽小組應確認矯正措施之執行結果，並評估改善計畫之預期效果向上呈報。

第十一章 附則

- 六十八、本要點於111年3月24日經董事會通過後實施，修正時亦同。