昆盈企業股份有限公司
KYE SYSTEMS CORP.

昆盈企業資訊安全政策

1. 目的：
   1.1. 強化資訊安全管理，確保企業資訊、系統、設備、網路通訊之安全，防止來自企業內外蓄意或非蓄意之破壞。
   1.2. 維持資訊系統持續運作，防止駭客、病毒入侵及破壞。
   1.3. 防止人為意圖不當及不法使用。
   1.4. 避免人為疏失意外。
   1.5. 維護實體環境安全。

2. 適用範圍：
   2.1 昆盈企業所屬各單位（含東莞）。
   2.2 人員、應用系統、硬體設備、網路設備及企業資訊等五個部份。

3. 名詞定義：

4. 權責
   4.1. 資訊部：負責資訊安全相關政策、計畫、措施及技術規範之研議，以及安全技術之研究、建置及評估相關事項。
   4.2. 稽核室：資訊安全稽核作業實施。
   4.3. 其他單位：資料及資訊機密保護執行。

5. 作業流程圖(略)

6. 作業內容

   6.1. 資訊安全政策制定及評估

      6.1.1. 資訊安全政策制定

         依證券交易法規定之「公開發行公司建立內部控制制度處理準則」第九條之法令規定及參考本公司實際業務需求。

      6.1.2. 資訊安全政策評估

         資訊安全政策應至少每年評估一次，以反應當前法令、技術及業務等最

新狀況。確保資訊安全作業之有效性。

6.2. 人員安全管理及教育訓練

6.2.1. 人員安全評估

6.2.1.1. 凡人員工作職責須使用或處理資訊者，應授與機密維護責任，並盡可能簽署書面約定，以明責任。

6.2.1.2. 人員離（休)職時，應立即取消使用企業內各項資訊資源之所有權限。

6.2.2. 資訊安全訓練

6.2.2.1. 新進員工教育訓練

人力資源處於新進員工教育訓練時，應同時說明企業資訊安全政策。

6.2.2.2. 定期宣導

6.2.2.2.1. 資訊部應於每半年以電子郵件公告宣導本資訊安全政策。

6.2.2.2.2. 其他經稽核察覺違反資訊安全政策之事項，得由資訊部定期公告。

6.2.2.2.3. 資訊部不定期以電子郵件公告現行病毒及駭客攻擊手法以提醒員工注意。

6.3. 電腦系統作業安全管理

6.3.1. 電腦系統作業程序及責任

6.3.1.1. 資訊硬體設備：設備進出機房需確實登記原因及承辦人員，新設備進入時需針對使用電力及網路做分配記錄。

6.3.1.2. Console：機房電腦管理管理畫面如無需使用須離開管理畫面，需設定當不使用系統時應於 5 分鐘內自動鎖定 Console。

6.3.1.3. 個人電腦:員工於公司內部使用個人電腦需由 資訊部協助安裝公司授權之防毒軟體及核發固定 IP 連接 AD(Microsoft Windows Active Directory) 網域控制站始可使用網路系統，除特別為公用定義之電腦外

均為個人使用之電腦，員工應對自己所屬電腦竭盡保管之責，並設定開機密碼，防止他人竊用。

6.3.1.4. 系統發展及實作分開管理：應將系統發展測試作業及系統正式作業之軟體，應盡量分別在不同處理器或不同的目錄下作業，以便系統測試與正式作業分開處理，並避免作業軟體或資料遭意外竄改，或不當使用。

6.3.1.5. 資訊委外安全管理：資訊業務委外時，應於事前審慎評估可能的潛在安全風險（例如資料或使用者通行碼被破解、系統被破壞或資料損壞等風險），與廠商簽訂適當的資訊安全協定，將相關的安全管理責任納入契約條款。

6.4. 軟體管理：

6.4.1. 使用合法授權軟體，未經授權合法之軟體，禁止使用。

6.4.2. 每半年至少公告一次，宣導企業對合法軟體使用之決心。

6.5. 日常作業之安全管理

6.5.1. 伺服器：每日需記錄伺服狀況及系統及 AP(應用系統)更新資訊(伺服器維護記錄表)。

6.5.2. 網路狀況：每日將網路狀況及預定的維護時程需登錄於網頁上供員工查詢(資訊部網頁)。

6.5.3. 密碼原則：資訊使用相關之各應用系統應設立密碼，並至少 90 天需更換密碼，且密碼不得少於 6 碼。

6.6. 電腦媒體之安全管理

6.6.1. 移動的電腦媒體，應建立使用管理程序，以規範磁帶、磁碟、光碟及電腦輸出表等媒體之使用，及相關因應措施。

6.6.2. 磁帶：如為備份重要企業資料之磁帶應編號列管，並將備份後之磁帶妥善保管於另一建築物中。

6.6.3. 光碟：光碟燒錄由每個部門主管自行依該部門需求管理燒錄之內容及數量。(部門主管指定人員負責登錄資料備查，並於每月前將上個月之記錄交附資訊部存查)

6.6.4. 行動碟及姆指碟之管理：禁止將公司機密等級以上相關資料複製於行動碟或姆指碟上及攜帶外出。(部門主管指定人員負責登錄資料備查，並於每月前將上個月之記錄交附資訊部存查)。

6.7. 網路安全管理

6.7.1. 網路安全規劃與管理

6.7.1.1. Firewall 管理：

6.7.1.1.1. 每日 Firewall 記錄檔檢視。

6.7.1.1.2. 發現異常入侵狀況需登錄於異常記錄表(Firewall 維護記錄表)，並當天呈報資訊部主管。

6.7.1.2. IP 發放原則：

6.7.1.2.1. 員工填寫 Internet 申請單時，如為新購電腦、更換使用或財產轉移，需由資訊部發放新 IP，並將該 IP 及 Mac Address 登錄於資訊部 IP 發放記錄表中，存查使用。

6.7.1.3. HUB：

6.7.1.3.1. 因新增電腦或設備導致網路端點無法滿足時可請求設立 HUB 以滿足所需，惟該 HUB 由需求部門申請採購(規格需由資訊部審核)，由資訊部協助安裝及設定。

6.7.1.4. 無線 AP(基地台)：

6.7.1.4.1. 資訊部統一設置企業用無線基地台及管理所有帳號及權限，嚴禁員工自行安裝 AP 及利用非資訊部認可之無線傳輸設備。

6.8. 電子郵件之安全管理

6.8.1. 電子郵件命名規則：

6.8.1.1. 電子郵件位址一律使用"英文名"_"英文姓"@geniusnet.com.tw

6.8.1.2. 如有特殊命名需求，如部門對外聯絡信箱，外籍員工等需於申請單上註明。

6.8.1.3. 於本文發行日前建立者無需異動。

6.8.2. 廣告信處理原則：

6.8.2.1. 進入公司之電子郵件皆經由信件內容過濾系統用以過濾非公務

相關之廣告信件。

6.8.2.2. 同仁如有發現未過濾之廣告信，可將該信轉由資訊部設定過濾條件。

6.8.3. 全體同仁信件之寄送：

6.8.3.1. 寄件目地人數達全公司一半以上者得使用全體同人帳號寄送。

6.8.3.2. 全體同仁帳號由資訊部網管人員管理寄送及內容過濾。

6.9. 全球資訊網之安全管理

6.9.1. 即時通(MSN)管理：

6.9.1.1. 僅開放 MSN,ICQ 等之即時通軟體文字對談功能，禁止傳檔及語音通話功能。

6.9.1.2. Skype 因尚無管理系統將禁止所有功能。

6.9.2. Web Mail(Yahoo,HotMail)管理

6.9.2.1. 禁止使用非公司提供之電子郵件系統。

6.9.3. FTP(檔案傳輸協定)

6.9.3.1. 由各部門主管管理該部門同人傳輸之檔案及其內容。(部門主管指定人員負責登錄資料備查，並於每月 2 日前將上個月之記錄交附資訊部存查)。

6.10. 區域網路資訊安全（東莞昆盈、長盈）：

6.10.1. 禁止自行設立 Server 及連外線路，所有異動需經台北資訊部管理確認方可執行。

6.10.2. ADSL：

各單位自行申請之 ADSL 測試用連外線路，禁止與公司內部網路連線，資訊部將不定期稽核其使用狀態以確保資訊安全。

6.10.3. 網路安全稽核

6.10.3.1. 作業系統漏洞修正

6.10.3.1.1. 凡使用電腦之人員應於接獲資訊部通知作業系統更新

事件時，應即時上網更新。

6.10.3.1.2. 當電腦送回資訊部維修時，資訊部當負責更新該 Patch 至最新狀態。

6.10.3.2. 病毒防制系統：

6.10.3.2.1. 凡連接於公司網路之電腦需有防毒軟體安裝，並且更新至最新病毒碼。

6.10.3.2.2. 公司使用之電腦將由資訊部統一安裝及維護該防毒系統。

6.10.3.2.3. 禁止員工自行卸載防毒系統，或未安裝防毒系統。

6.10.3.2.4. 外來訪客禁止自行連接公司網路，如有需要，須向資訊部提出申請。

6.10.4. 系統存取控制

6.10.4.1. 網路存取之安全控制

6.10.4.1.1. 檔案分享：

6.10.4.1.1.1. 資訊部提供一檔案伺服器,每日備份等機制供各部門存放該部門公用檔案。

6.10.4.1.1.2. 每個部門可申請一部門目錄，需自行定期整理，避免非必要性檔案佔用空間。

6.10.4.1.1.3. 預設為 50MB，如有特別需求可另案提出申請。

6.10.4.1.2. 對外 FTP

6.10.4.1.2.1. 提供連外之檔案交換，相關規定如"檔案分享"。

6.10.4.1.3. 網路芳鄰：

6.10.4.1.3.1. 個人電腦開啟磁碟共享之機制,須由開放之個人負責自行電腦之存取權限及安全。

6.10.4.1.3.2. 由於頻寬限制，非同一建築物間網路將禁止使用"網路芳鄰"功能。

6.11. 應用系統之存取控制

6.11.1. ERP2

6.11.1.1. 帳號申請：員工填寫”ERP2 帳號申請單”經由部門主管同意，資訊部模組負責人及資訊部主管審核後開放。

6.11.1.2. 帳號取消：資訊部接到員工之”離職申請書”後即刻停止該帳號使用權。

6.11.1.3. 權限異動：員工填寫”ERP2 權限異動單”，經由部門主管同意，跨部門主管同意(如有其它模組需求)，資訊部模組負責人及資訊部主管審核後開放。

6.11.2. eHR：

6.11.2.1. 由人力資源處負責帳號及權限管理維護，主機系統置於資訊部機房統一管理。

6.11.3. eProcurement：

6.11.3.1. 帳號申請：員工填寫” eProcurement 申請單”(廠商申請由;資材部代為申請)經由部門主管同意，資訊部模組負責人及資訊部主管審核後開放。

6.11.3.2. 帳號取消：資訊部接到員工之”離職申請書”後即刻停止該帳號使用權。

6.11.4. PLM

6.11.4.1. 帳號申請：員工填寫” TSD 網路申請單”經由部門主管同意，OEM TSD-PLM 負責人及經理審核後開放。

6.11.4.2. 帳號取消：OEM TSD 之 PLM 管理者須於接到員工之”離職申請書”後即刻停止該帳號使用權。

6.12. 系統發展及維護之安全管理

6.12.1. 在作業系統上執行應用軟體，應建立控制程序並嚴格執行，為減少可能危害作業系統的風險，作業用的應用程式更新作業，應限定只能由授權的管理人員才可執行，且應建立應用程式的更新稽核記錄。

6.12.2. 作業用的應用程式均應以目的程式為原則；除非核准，不得以原始程式作業。

6.12.3. 系統測試資料之保護：

6.12.3.1. 應保護及控制測試資料，避免以正式環境的資料庫進行測試；如使用正式環境的資料進行測試時，應於事前將足以辨識個人的資料變更。

6.12.3.2. 測試完畢後，正式環境資料應立即從測試系統中刪除。

6.12.3.3. 正式環境資料的複製情形予以記錄，以備稽核運用。

6.12.4. 系統變更及維護環境之安全

6.12.4.1. 應用系統變更(修改)作業之控制程序

6.12.4.1.1. 應依循變更(修改)控制程序，並嚴格執行，以降低可能的安全風險；變更作業之控制程序，應確保系統安全控制程序不會被破壞，並確保程式設計人員只能存取系統作業所需的項目，且任何的系統變更作業，皆應獲得資訊部主管的同意。

6.12.4.1.2. 應依事前訂定的授權規定，執行變更(修改)作業，其控制程序應考量的事項：

6.12.4.1.3. 在實際執行變更作業前，變更作業的細項建議，應取得權責主管人員之核准。

6.12.4.1.4. 系統文件在每次完成變更作業後，應立即更新，舊版的系統文件亦應妥善保管及處理。

6.12.4.1.5. 系統文件應有版別及啟用日期之識別。

6.12.4.1.6. 所有的系統變更作業請求，皆應建立紀錄供稽核運用。

6.12.4.2. 作業系統變更之技術評估：

6.12.4.2.1. 作業系統更新前應評估其對應用系統是否造成負面的影響，或產生安全問題。

6.12.4.2.2. 作業系統變更的評估及測試結果，如須進行必要的調整，應納入年度計畫。

6.12.4.3. 系統維護環境之安全控管

6.12.4.3.1. 軟體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。

6.12.4.3.2. 核發短期及臨時性之系統辨識及通行密碼供廠商使

用，於使用完畢後應立即取消其使用權限。

6.12.4.3.3. 委外廠商建置或維護軟硬體設施時，應在資訊部相關人員陪同下為之。

6.13. 實體及環境安全管理

6.13.1. 備份系統管理：

6.13.1.1. 核心系統(ERP、Files)需每日備份。

6.13.1.1.1. 備份原則：

6.13.1.1.1.1. 每日差異備份，每週或每月一次的全備份(Full Backup)。

6.13.1.1.1.2. 每日需查驗備份記錄。

6.13.1.2. 媒體管理：

6.13.1.2.1. 每份媒體均須編號及列管。

6.13.1.2.2. 媒體啟用及報廢均需記錄。

6.13.1.2.2.1. 報廢時須徹底毀損媒體，確保無法讀取及使用。

6.13.1.2.2.1.1. 光碟、磁碟之毀損須使用裁切段或燒毀。

6.13.1.2.2.1.2. 磁帶之毀損須拉出磁帶燒毀。

6.13.1.2.2.2. 累積一段時間做資訊總整理時,須特別注意有否大量非機密性資料彙總成機密性資料。

6.13.1.2.3. 年度每月之全備份需攜出於異地存放。

6.13.1.2.4. 媒體存放處需有防潮及上鎖裝置。

6.13.1.3. 復原機制：

6.13.1.3.1. 每半年一次復原演練。

6.13.1.3.2. 如復原過程或結果不盡理想，應馬上執行全備份，並重新復原演練。

6.14. 機房安全管理

6.14.1. 電力系統：與辦公室分離之獨立之電源系統，及 UPS 不斷電系統，搭配專用發電機組。UPS 每組輸出電力需每日記錄，電力使用不得高於每組最高供給電力 75%以上。UPS 電池需於 2 年置換一次，並簽定維護合約

定期保養。

6.14.2. 消防系統：設置二氧化碳滅火器(電子設備使用)，以確保滅火時將設備損傷降至最低。

6.14.3. 獨立之空調系統，保持攝氏 20~30 度，濕度 50~60%，並每日記錄。

6.14.4. 人員進出管制：已授權之經常性作業人員進出機房需刷卡進入門禁，除外人員進出需於門禁管制表登記。有刷卡授權人員一但離職，需立即取消門禁系統之權利。

7. 控制重點

7.1. 本資訊安全政策應至少每年評估一次，以反應政府法令、技術及業物等最新發展狀況，確保資訊安全實務作業之有效性。