一通數位資訊管理辦法

壹.主旨：

為強化本公司資訊安全管理，確保資料、系統、設備及網路安全，特訂定本辦法。

貳.目的：

1.制訂電腦軟體使用之規定，防止因違反著作權法而損及公司利益。

2.制訂資訊安全政策，防止機密或敏感資訊外流。

3.制定災害復原計畫，保障災害時之系統回復性。

參.範圍：本規章適用於各公司之所有人員與資訊設備。

肆.權責：

1.運維或執行資訊相關業務人員需依本規章之規定，實施相關之措施，確保公司資訊安全政策之落實。

伍.作業內容：

1.軟體與系統使用之規定：

(1)嚴禁於公司電腦中使用或安裝未經合法授權之電腦軟體。

(2)相關工具軟體規範已制定於confluence

(3)嚴禁非法複製軟體給笫三者(包括但不限於同事、客戶及顧客)。

(4)密碼應以亂碼方式儲存,個人電腦應開啟螢幕保護及鎖定密碼之功能。

(5)使用個人電腦若因業務需求，需要安裝特定之電腦軟體，應提出申請。

(6)個人電腦應開啟螢幕保護及鎖定密碼之功能。

(7)若有特殊權限需求，申請人應提出申請， 載明特殊需求原因，並經權責主管核准後交由運維主管執行設定。

(8)正式運營環境的操作，須由兩位運維協同操作，操作時由另外一位運維告訴指令，審核後執行操作AB覆核式指令操作。

2.電腦使用之規定：

(1)安裝合法授權之工具軟體供員工使用。

(2)應使用個人帳號登入，以識別使用者權責，並嚴禁將個人檔案存入硬碟中。

3.資訊安全管理事項：

(1)資訊存取管理：內網內所有電腦終端設備及個人電腦設備之資料存取裝置，包含但不限於光碟機及各式卸除式裝置，使用者若有業務上之需求，需與權責單位申請。

(2)資訊相關帳號管理：

(a)公司相關帳號:  
員工新進時，由部門主管協助提出申請，經權責主管核准後，交運維權責人員開通帳號；員工離職時，依本公司離職作業程序會簽至運維主管後，由該權責人員關閉其帳號。

(b)使用者應適時且定期更換密碼，以降低資安風險。

(c)授權所有帳號使用密碼者應造冊列管，密碼應定期更換，個人之密碼不得借他人使用。

(d)員工離職或是調離其職位時，曾經手之一切文件、磁碟片、光碟片、所有帳號清冊等均須盤點且清楚辦理移交手續

(e)員工離職或是調離其職位時，所接觸或使用之帳號及密碼均應作更改調整

(f)對於已遞交辭呈之員工，立即避免離職前接觸敏感或機密性程式或檔案，當下立即停止正在處理之計畫並交接給適當代理人。

(3)應使用合法授權軟體，委外開發之資訊軟體系統，需取得相關廠商授權合約書，合約內容應包含資料保密協議條約。

(4)電腦病毒防護：

(1)防毒軟體隨時更新病毒碼。

(2)新購入之各式個人電腦主機、伺服器主機、控制儀器或機台之電腦主機等具備資訊電腦作業系統介面之相關設備， 需完成下列相關驗收程序方能上線連接內網：

(a)檢查電腦作業系統(Computer Operating System)是否完成最新之安全性更新(WindowsUpdate)。

(b)掃描磁碟機等等確認無隱藏電腦病毒。

(c)防毒應涵蓋個人端及網路伺服器端電腦。

(d)外來資料隨身碟需先經使用者防毒偵測

(e)火牆應由運維主管執行控管設定。

(3)所有運行中的電腦主機應定期執行防毒軟體掃毒程序及作業。

(5)資訊安全事件通報：

(1)員工或相關人員發現資安事件時應即時向運維或管理部機關反映，再交由運維部進行處理。

(a)重要資料發現外洩時，如：個人資料、研發及技轉資料..等。

(b)系統遭受外部攻擊，導致資料毀損或無法開啟。

(c)系統中毒。

(d)伺服器資源不當佔用時。

(e)資安系統發出異常警示報告時。

(f)因其他不明原因，造成資料、設備毀損或營運中斷時。

(2)事件嚴重等級區分為三級：第三級(輕度)：影響度僅為個人，第二級(中等)：影響度已達該部門，第一級(重度)：影響度擴及其他部門或重要機密資料外洩。

(c)第三級c:資安事件僅影響個人電腦及其作業時， 例如操作錯誤、個人作業資料或設備毀損等，通報人應申請且處理復原。

(b)第二級b:資安事件判斷為非機密資料之毀損或外洩足以造成部門作業中斷，並無法於可容忍中斷時間內回復正常運作，通報人應填寫通管理部最高主管。

(a)第一級a:事件判斷為機密資料之毀損外洩或者生產環境故障不可用時，通報人應通報運維、管理部最高主管及相關權責人員。

(3)如遇緊急資安狀況應立即以口頭或訊息通報相關權責主管，以加強處理時效，由通報單位填寫交由運維人員註明其處理

4.網路安全管理：

(1)基礎設施建置：

(a)架設防火牆：應避免外部網路直接連通公司內部網路，防火牆配置應符合網路安全架構，僅提供必要使用之安全通道vpn，並關閉其他非必要之通道。

(b)設置入侵偵測系統：偵測及紀錄外部入侵跡象，控管遭受外部入侵風險，應定期檢視入侵防護報告至權責主管覆核。

(2)防火牆管理：

(a)防火牆設定規則內容應依據公司(辦公室所合法登記之實際 IP 進行連線設置，各部門若有非屬公司合法登記之外部 IP 連線需求，應申請經權責主管核定後，交由運維設置防火牆連線等等。

(b)防火牆由外部連入之 IP 通道(port)，依據最基本網路服務性質開通，例如網站服務為 HTTP、HTTPS、FTP，網域服務 DNS，電子郵件服務POP3、SMTP、IMAP，遠端連線服務 VPN，員工考勤服務等，若內部或無上述非相關工作服務則應保持關閉相關 IP 通道等，若各部門有特殊 IP 通道需求需要開放，應提出申請經權責主管核定後，交由運維人員設定。

(2)連網安全規範：

1.公司本地端連網服務(Local)，應區分內網及外網， 內網為提供公司內部資料存取之通道網絡，外網為提供客戶及一般無線裝置上網服務，外網不可直接連通內網。

2.遠端(Remote)連網辦法：

應透過企業自有或合法租用之私密連線及加密機制(VPN) 與企業內部網路連線。

(a)使用遠端連網連通外部網路與公司內網，僅限運維權責人員及經授權之員工。

(b)因業務需求或公司內員工，必須透過遠端連網進行資料串連作業者，應提出申請，並經權責主管核准後，交由運維執行遠端連網開通。

(c)使用遠端連網之裝置，應為公司內部合法註冊之資訊設備，或經權責主管核准使用之資訊通訊設備。

(d)使用第三方遠端連網軟體僅限於運維等人員進行遠端協助海外公司或公司外地廠區、辦公室之資訊服務及有簽訂維護(含保密)合約之資訊系統廠商進行即時系統問題排除作業，其他一律禁止使用。

(3)網路安全管理：

1.公司網站(WWW)為放置公開資訊之網站，不得存放機密性資料。

2.使用公司檔案傳輸網站(FTP)，應取得權責主管核准，採具名帳號登入存取，並嚴格禁止私人檔案傳輸。

3.因業務需求，需經由全球資訊網路傳輸公司機密性資料 時，應使用經安全加密機制之網路傳輸。所使用之安全加密機制，應取得網路公正第三方認證之安全加密機制。

4.應定期評估自身網路系統安全。

5.定期或適時修補網路運作環境之安全漏洞及宣導有關電腦網路安全事項。

6.各電腦主機重要軟硬體設備應有運維部負責。

7.資料經由電子郵件傳送或接收時，應於電腦系統設置防火牆及防毒軟體以防駭客或電腦病毒之侵害。

(4)員工上網行為管理：

1.嚴禁員工使用網路下載非法軟體。

2.嚴禁員工利用公司網路散佈非法或色情之軟體、聲音、圖片及文字。

3.嚴禁員工利用公司網路連線非自身工作業務範圍之網路服務，包含挖礦、網路遊戲、雲端硬碟、網路社群媒體、網路直播等等連線。

4.嚴禁員工使用公司網路瀏覽色情網站。

5.嚴禁員工利用公司網路從事侵入其他公司或機關組織之網路或其他非法入侵網路行為。

5.災害復原計畫：

為因應各種天然災害或人為意外，造成公司資訊資產損害，應備妥完整資訊資產復原方案，以降低公司損失。

1.資訊系統備份作業：

(1)資訊系統包含資訊內容檔案之備份，依據下列方式作業

(a)異機備份：將主要資訊系統及資料內容之備份檔案，定期備份至本地端之其他伺服器內，例如備援伺服器內。

(b)異地備份：將主要資訊系統及資料內容之備份檔案，定期備份至公司外部安全存放地點。

上開作業若為自動化備份應定期輸出自動備份，並告知權責機關

(2)防火牆配置檔應於每次更新後下載備份。

(3)將重要系統檔案、程式及資料檔案定期進行備份。

(4)備份檔案應適當命名，以利辨識備份內容。

(5)備份檔案不得借調。

2.資訊系統還原作業：

(1)系統還原：藉由章節第伍.5.1.(1)之備份作業，可將資訊系統備份檔， 進行系統還原。

(2)還原測試：每年不定期執行各主要之資訊系統還原測試一次，以驗證備份之有效性。

3.資訊設備備援：

(1)電力備援：電腦機房應備妥充足電力之不斷電系統，以防止環境電力中斷，造成機器設備毀損。

(2)數據網路線路備援：電腦機房應配置 2 條以上，相同頻寬之對外數據網路連線，以達到相互備援之功能。

(3)資訊系統伺服器備援：重要資訊系統應配置主要伺服器及備援伺服器或這快照鏡像之異機備援架構，於主要伺服器故障時，備援伺服器可取代執行資訊系統運作。

6.資訊設備收回作業：

1.收回時機：資訊人員應於下列時機收回公司配發予個人之資訊產品。

(a)員工離職：應於辦妥離職手續前，歸還公司配發予個人之資訊產品。

2.收回驗收：收回之資訊產品應先檢驗該設備是否功能正常，若有明顯之人為損壞，應依照負維修賠償之責任。

陸. 資訊支援及服務：

1.運維單位取得業務請求後，應配合需求時間完成處理，若無法即時完成，應與需求單位溝通並取得共識。

2.相關使用單位如因業務需要，需調閱相關資料時，應提出申請，經權責主管核准後始得調閱。

柒.資訊管理政策之宣導及罰則：

1.若發生資訊安全事件，應先向運維人員通報。該人員先採取適當反應措施後記錄。若有情節重大者，則聯繫檢警調單位協助偵查。

2.若發現未經適當核准而外流公司資料檔案者，公司得依情節重大及對公司之損害程度，懲處相關員工或進行索賠。

捌.本辦法經管理部核准公告後施行，修正時亦同。