修定明細 / 制(修)訂單位 ： 資訊部

Date	Rev	Page No	Description of Change	改版人	備註
1040508	1.0	ALL	新發行	葉津村	
1070420	2.0	ALL	全面重新檢視修訂	陳厚銘	
1070814	2.1	3、6	5.3.4 修訂、5.8 增訂	陳厚銘	
1080102	3.0	ALL	全面重新檢視修訂	陳厚銘	
1080725	3.1	1、2、4、5、7、8、9、12	5.1.7 修訂、5.1.8 修訂、5.3.4.1 修訂、5.3.4.3 修訂、5.4.2.2 修訂、5.4.2.2.1 修訂、5.4.2.2.4 增訂、5.5.1.1 修訂、5.5.1.2 整併、5.5.2.1 修訂、5.5.2.2 修訂、5.5.3.3 增訂、10 修訂	陳厚銘	
1081220	3.2	1、2、3、4、7、8、9、10、11	5.1.3 刪除、5.1.5 修訂、5.1.7 修訂、5.1.9 修訂、5.3.1.2 修訂、5.3.2.1 修訂、5.3.2.2 修訂、5.3.4.1 修訂、5.3.6 修訂、5.5.1.1 修訂、5.6.2 修訂、5.8.2 修訂、5.11 修訂、5.11.1 修訂、5.11.2 修訂、5.11.3 修訂、6.3 修訂、7 修訂、9 修訂	陳厚銘	
1090206	3.3	8	5.6.2 修訂	陳厚銘	
1090907	3.4	7	5.5.1.1 修訂	陳厚銘	
1100319	3.5	2	5.1.10 增訂	陳厚銘	
1110303	3.6	5、6	5.6 修訂、5.6.3 增訂、5.6.4 增訂	陳厚銘	
1111227	3.7	3、8	5.3.2.3 修訂、5.5.1.1 修訂、5.5.1.3 修訂	陳厚銘	
1120316	3.8	7	5.5.1.1 修訂	陳厚銘	
1120609	3.9	2	5.1.10 修訂	陳厚銘	

1.目的：

1.1 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。

1.2 制訂資訊安全政策，防止機密或敏感資訊外流。

1.3 制定災害復原計畫，保障災害時之系統回復性。

2.範圍：本規章適用於集團內各公司之所有人員與資訊設備。

3.權責：

3.1 資訊部或子公司執行資訊相關業務人員：

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。

3.2 非資訊部人員：

確實遵守公司資訊安全政策及電腦軟體使用之規定。

3.3 核准層級與流程均載明於本規章 11.作業表單上。

4.定義：無

5.作業內容：

5.1 個人電腦軟體使用之規定：

5.1.1 嚴禁於公司電腦中使用或安裝未經合法授權之電腦軟體。

5.1.2 嚴禁非法複製軟體給第三者(包括但不限於同事、客戶及顧客)。

5.1.3 員工個人密碼僅供個人使用，並需妥善保存，輸入錯誤超過 5 次時，系統將自動鎖定帳號，使用者應通知資訊部協助處理。

5.1.4 員工使用 ERP 時，需依照個人工作執掌，填寫【資訊系統權限使用申請表】及【ERP 模組權限表】，申請新增或修改使用權限，經權責主管核准後，交由資訊部執行 ERP 程式安裝及帳號權限設定。非員工需使用 ERP 時，需由負責接待之窗口提出申請，並註明使用起訖之時間經權責主管核准後交由資訊部開通其 ERP 權限，並於申請時間到期後關閉此非員工帳號。

5.1.5 員工需簽署【電腦軟體使用切結書】，並遵守相關規範。

5.1.6 員工使用個人電腦若因業務需求，需要安裝特定之電腦軟體，應填寫【資訊設備軟硬體使用申請表】，經權責主管核准後，交由資訊部執行軟體安裝。

5.1.7 個人電腦作業系統登入密碼原則：

(1)每 90 天變更密碼 1 次。

(2)密碼最小長度為 8 字元。

(3)必須符合密碼複雜度。密碼複雜度是指密碼必須包含下列四種字元其中之三種以上種類字元：一、英文大寫字元 (A 到 Z)。二、英文小寫字元 (a 到 z)。三、數字 (0 到 9)。四、半形符號字元 (例如: !、$、#、%)

5.1.8 個人電腦應開啟螢幕保護及鎖定密碼之功能。

5.1.9 若有特殊權限需求，申請人應填寫【資訊系統權限使用申請表】，載明特殊需求原因，並經權責主管核准後交由資訊部執行設定。

5.1.10 員工應使用公司合法配發之電腦設備處理公務，並妥善保存職務工作相關之電子檔案於該電腦磁碟內，除有特殊事由且獲總經理簽核核准外，禁止使用私人電腦（包括但不限於筆電、平板）及電子信箱處理公務。

5.1.11 員工使用印表機，應設定黑白列印為預設值，若有列印彩色需求再手動變更設定。

5.2 公用電腦使用之規定：

5.2.1 安裝合法授權之工具軟體供員工使用。

5.2.2 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。

5.3 資訊安全管理事項：

5.3.1 資訊存取管理：

5.3.1.1 網域群組管理：

所有公司資產之電腦終端設備及個人電腦設備，均應加入企業網域群組(以下簡稱內網)。

5.3.1.1.1 內網內所有電腦終端設備及個人電腦設備軟體之使用，應依 5.1 之規定辦理。

5.3.1.1.2 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，得填寫【資訊設備軟硬體使用申請表】，申請解除管制。

5.3.1.1.3 非公司資產之個人電腦設備嚴禁連接內網。

5.3.1.2 電子檔案管理：

區分機密性與一般性。

5.3.1.2.1 機密性電子檔案管理：依據『營業秘密管理辦

法』內載明之相關規定辦理。

5.3.1.2.2 一般性電子檔案管理：依據各部門權限流通管理及個人自行運用管理，惟個人電腦設備依本規章 5.1.8 進行密碼管制。

5.3.2 資訊相關帳號管理：

5.3.2.1 公司網域帳號：

員工新進時，由部門主管協助提出申請，經權責主管核准後，交由資訊部權責人員開通帳號；員工離職時，依本公司離職作業程序會簽至資訊部後，由資訊部權責人員關閉其帳號。

5.3.2.2 電子郵件帳號：

員工新進時，由部門主管協助提出申請，經權責主管核准後，交由資訊部開通帳號；員工離職時，依本公司離職作業程序會簽至資訊部後，由資訊部刪除其帳號。若需保留離職員工之電子郵件帳號，需於員工完成離職程序前，填妥【資訊系統權限使用申請表】，並經權責主管核准後，交由資訊部辦理保留作業。該保留期限以二個月為原則，若未提出申請展延，屆期由資訊部逕自刪除帳號。

5.3.2.3 其他帳號：

包含 ERP、電子簽核、報表系統、文件管理系統、文件加密系統等，處理程序同 5.3.2.1。

5.3.3 應使用合法授權軟體，委外開發之資訊系統，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。

5.3.4 電腦病毒防護：

5.3.4.1 應購買足敷使用之防毒軟體，並隨時更新病毒碼。

5.3.4.2 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：

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

5.3.4.1.2 掃描磁碟機確認無隱藏電腦病毒。

5.3.4.1.3 安裝最新版本之防毒軟體。

5.3.4.3 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。

5.3.5 公司內部資訊系統主機，得於排定系統維修日或休假日期間，經公告後，關閉主機資料存取服務，降低受駭機率。

5.3.6 各部門 ERP 使用者若有職務異動時應填寫【資訊系統權限使用申請表】重新申請符合異動後職務之 ERP 使用權限送交相關權責主管覆核，再由資訊部權責人員進行調整。

5.3.7 資訊安全事件通報：

5.3.7.1 員工發現資安事件時應即時向資訊部反映，並依據資安事件之嚴重程度，分由不同之權責人員核定，再交由資訊部進行處理。

5.3.7.1.1 重要資料發現外洩時，如：個人資料、研發及技轉資料..等。

5.3.7.1.2 系統遭受外部攻擊，導致資料毀損或無法開啟。

5.3.7.1.3 系統中毒。

5.3.7.1.4 伺服器資源不當佔用時。

5.3.7.1.5 資安系統發出異常警示報告時。

5.3.7.1.6 因其他不明原因，造成資料、設備毀損或營運中斷時。

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

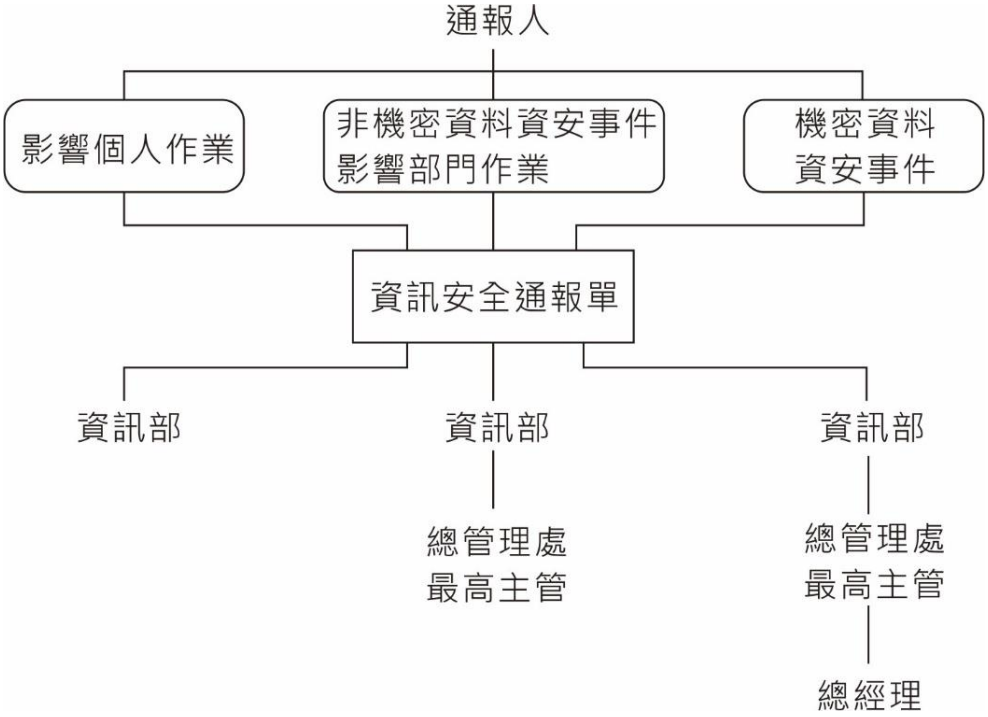
5.3.7.2.1 第一級：資安事件僅影響個人電腦及其作業時，例如操作錯誤、個人作業資料或設備毀損等，通報人應填寫【資訊安全事件通報單】，直接交由資訊部協助處理復原。

5.3.7.2.2 第二級：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【資訊安全事件通報單】通報資訊部及總管理處最高主管。

5.3.7.2.2 第三級：資安事件判斷為機密資料之毀損或外洩時，通報人應填寫【資訊安全事件通報單】通報資訊部、總管理處最高主管及總經理。

5.3.7.3 如遇緊急資安狀況應立即以口頭或 Email 通報資訊部主

管，以加強處理時效，由通報單位填寫【資訊安全事件通報單】，經權責單位主管核准後，交由資訊部註明其處理措施後，定期追蹤檢查其改善方式有效性，避免資安事件再次發生。



資安事件通報流程圖

5.4 網路安全管理：

5.4.1 基礎設施建置：

5.4.1.1 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(Lan Port)，並關閉其他非必要之通道。

5.4.1.2 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後 Email 傳送相關報告至權責主管覆核。

5.4.1.3 防火牆管理：

5.4.1.3.1 防火牆設定規則內容應依據公司(包含集團內各子公司)辦公室、工廠所合法登記之實際 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，應填寫【資訊系統權限使用申請表】經權責主管核定後，交由資訊部設置防火牆連線。

5.4.1.3.2 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，若內部無上述相關服務則應保持關閉相關 IP 通道，若各部門有特殊 IP 通道需求需要開放，應填寫【資訊系統權限使用申請表】經權責主管核定後，交由資訊部設定。

5.4.2 連網安全規範：

5.4.2.1 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，外網不可連通內網。

5.4.2.2 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。

5.4.2.2.1 使用遠端連網連通外部網路與公司內網，僅限資訊部權責人員及經授權之員工。

5.4.2.2.2 因業務需求或集團內員工，必須透過遠端連網進行資料串連作業者，應填寫【資訊系統權限使用申請表】，並經權責主管核准後，交由資訊部執行遠端連網開通。

5.4.2.2.3 使用遠端連網之裝置，應為集團內公司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。

5.4.2.2.4 使用第三方遠端連網軟體僅限於資訊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。

5.4.3 全球資訊網路(Internet)安全管理：

5.4.3.1 公司網站(WWW)為放置公開資訊之網站，不得存放機密性資料。

5.4.3.2 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。

5.4.3.3 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。

5.4.4 員工上網行為管理：

5.4.4.1 嚴禁員工使用網路下載非法軟體。

5.4.4.2 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。

5.4.4.3 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。

5.4.4.4 嚴禁員工使用公司網路瀏覽色情網站。

5.4.4.5 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。

5.5 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。

5.5.1 資訊系統備份作業：

5.5.1.1 資訊系統包含資訊內容檔案之備份，依據下列方式作業

5.5.1.1.1 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。

5.5.1.1.2 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設定自動發送備份結果之通知予資訊主管，若為人工備份應填載【資料備份紀錄表】並由資訊部主管定期抽檢及覆核。

5.5.1.2 防火牆配置檔應於每次更新後下載備份。

5.5.1.3 電子郵件備份：公司電子郵件應即時備份於雲端伺服器租用空間，雲端租用空間安全存量低於 20%時應下載超量之郵件，儲存於公司內部檔案伺服器內，電子郵件備份檔保存期限為 1 年。

5.5.2 資訊系統還原作業：

5.5.2.1 系統還原：藉由 5.5.1.1 之備份作業，可將資訊系統備份檔，進行系統還原。

5.5.2.2 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。

5.5.3 資訊設備備援：

5.5.3.1 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。

5.5.3.2 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。

5.5.3.3 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。

5.6 資訊資產購置與報廢作業程序：

5.6.1 資訊設備如因故障、閒置、遺失、老舊功能效率不佳等原因需提報廢時，應由保管單位填寫【固定資產異動申請表】，說明原因並呈總經理核准後，併同【固定資產異動申請表】轉財務部會簽報廢、銷帳，再將【固定資產異動申請表】轉交管理部，辦理變更登錄作業。

5.6.2 資訊設備報廢後，若內接之儲存裝置尚未故障或毀損，應將內存之使用者個人工作檔案予以永久刪除，並尋求出售。若為無出售價值之資產設備，應予實體破壞，並於【固定資產異動申請表】註明處理之情況，以留存報廢紀錄備查。

5.6.3 資訊設備之新購應由需求單位填寫 ERP 內之【資產請購資料建立作業】表單進行請購簽核，且須符合下列條件：

5.6.3.1 新進人員已無閒置堪用電腦可配發者。
5.6.3.2 汰舊換新：設備使用年限已達公司法定之攤提年限者。
5.6.3.3 特殊業務需求。
5.6.4 資訊設備之採購由公司內部專職採購人員主辦採購之作業，並由資訊部協助規格審查之會辦，規格審查須符合下列原則。
5.6.4.1 以符合公司內部資訊網路環境相容之規格。
5.6.4.2 以「一機體(All In One)」為原則，避免主機必需使用轉接頭、轉接線方能正常使用之規格。

5.7 電腦機房管理：
5.7.1 門禁管理：
除總管理處主管及資訊部權責人員外，其他人員不得進入電腦機房。若因外部廠商需要進入電腦機房安裝設備、網路、電路、空調、內部裝修等工程作業或其他員工需要進入電腦機房執行工作業務，應由資訊部人員陪同，並於【電腦機房進出登記表】登載進入人員之單位及姓名、陪同人員之姓名及進出時間、進出事由以備查。
5.7.2 機房環境及設備管理：
5.7.2.1 資訊人員應每日進行機房環境及設備狀況檢視，並紀錄於【資訊機房日誌】。
5.7.2.2 機房配備之溫濕度紀錄器應定期輸出溫濕度紀錄報表，由資訊部主管覆核。

5.8 資訊產品收回作業：
5.8.1 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。
5.8.1.1 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。
5.8.1.2 設備更換：員工申請更換資訊產品時，需於收到更換品之3日內歸還被更換品。
5.8.1.3 借用歸還：應於約定借用之期限內歸還。
5.8.2 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『固定/列管資產管理辦法』之規定負維修賠償之責任。

5.9 資訊資產委外送修作業：

資訊資產若因故障、損壞，經資訊人員判定無法自行修復，例如：零件、外殼、韌體等損壞狀況，需要委外(原廠)送修時，需填寫【委外送修紀錄表】以追蹤委外送修進度。廠商送回資訊資產時，資訊人員應於【委外送修紀錄表】內紀錄修復或不能修復之狀況說明。

5.10 資訊資產清單管理：應編列主要資訊系統之【資訊資產清單】，例如應用程式系統伺服器、檔案伺服器、網通設備伺服器、儀控電腦等，編列【資訊資產清單】需註明資產編號、取得年份、資產規格、保管人、使用單位及風險評估，並於資訊資產異動時更新【資訊資產清單】內容。

5.11 資訊資產風險評鑑：資訊資產應依據資產購入年份、安全容量、妥善狀況、資訊環境相容度等條件評鑑資訊資產風險為高、中、低3級，並將評鑑結果登錄於【資訊資產清單】內。

5.11.1 若符合下列條件任3項之資訊資產應列為為高風險：

(1)購入年份超過6年。

(2)安全容量低於20%。

(3)妥善狀況不佳(例如部份主要零組件故障，已無零件可更換，但尚能開機運作)。

(4)資訊環境相容度低(例如：主流資訊廠商停止支援之系統，如WINXP、WIN2003以前版本及這些版本相容之應用程式)。

5.11.2 若符合下列條件任3項之資訊資產應列為中風險：

(1)購入年份超過3年未達6年。

(2)安全容量尚介於50%至20%之間。

(3)妥善狀況尚可(無零件損壞或有零件損壞但經過更換新零件等紀錄)。

(4)資訊環境相容度尚能相容(例如：主流資訊廠商尚未停止支援之系統)。

5.11.3 若符合下列條件任3項之資訊資產應列為低風險：

(1)購入年份未超過3年。

(2)安全容量尚餘50%以上。

(3)妥善狀況佳(無零件損壞紀錄)。

(4)資訊環境相容度高(例如：主流資訊廠主要推薦之系統)。

6.資訊支援及服務：

6.1 員工個人電腦發現異常，資訊單位檢視無法即時完成處理或需其他支援服務(如：程式修正等)，由需求人員填寫【資訊支援申請表】，經權

責主管核准後交由資訊單位辦理。

6.2 資訊單位取得上述申請後，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。

6.3 海外子公司之各項資訊支援及服務，需要資訊部派員協助時需填寫【資訊支援申請表】，經權責主管核准後，交由資訊部執行支援服務，資訊人員得視情況以遠端軟體或指導當地人員協助處理，若需派員，資訊單位需依『國內外出差管理辦法』執行，另相關費用依『關係人交易之管理』辦法予以計收。

7.資訊管理政策之宣導及罰則：

7.1 資訊部門應定期宣導本規章之資訊政策規範或相關之資訊安全教育訓練，以提高員工正確使用資訊科技知識及敦促員工遵守資訊安全規範。

7.2 違反本規章規定之員工，得依『人事管理規則』第三十七條之規定施行罰則。

8.本規章經董事長核准後實施，修改時得授權總經理核定。

9.相關文件：

9.1 營業秘密管理辦法
9.2 關係人交易之管理
9.3 國內外出差管理辦法
9.4 人事管理規則
9.5 固定列管資產管理辦法

10.參考資料：

空白 ERP 模組權限清單
(http://m1.metatech.com.tw/PUBFILE/pubfilelist.aspx?fk=MIS 表格)

11.作業表單：

11.1 資訊系統權限使用申請表
11.2 電腦軟體使用切結書
11.3 資訊設備軟硬體使用申請表
11.4 電腦機房進出登記表
11.5 資訊支援申請表
11.6 資訊機房日誌

11.7 委外送修紀錄表
11.8 資訊安全事件通報單
11.9 資料備份紀錄表
11.10 資訊資產清單