制訂日期	JUN.02.2006	文　　件　　名　　稱	頁次	核　發　章
文件編號	2136	集團資訊安全管理辦法	1	
版本、版次	1.2			

壹・目的：

胡連集團為強化資訊安全管理，確保所屬之資訊資產、系統環境、電磁資料的機密性、完整性及可用性，以提供集團內資訊運作所需之環境與架構，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，特制定此政策規範供所有從業人員參考並遵循。

貳・範圍：

凡屬集團內所有資訊系統、環境、操作、管理等相關人、事、物；包含全體員工皆應嚴格遵守本規範。

參・權責單位：

1. 資訊安全政策、計畫以及技術規範之研議、建置與評估等事項，由營運中心資訊室主導負責並會同各廠區資訊單位協助辦理。
2. 資料及資訊系統之安全需求研議、使用管理及維護等事項，由使用單位或業務承辦單位負責辦理。
3. 資訊安全之稽核作業，由稽核室會同資訊室負責辦理。

肆・參考資料：

一、1E001-電腦化資訊系統處理循環。
二、2012-電腦硬、軟體管理辦法。
三、2020- ERP 系統使用者權限管理辦法。
四、2114-應用系統密碼管理辦法。
五、2133-電子郵件管理辦法。

伍・定義：

1. 資訊安全管理係保護資訊資產，避免遭受各種不當使用、洩漏、竄改、竊取、破壞等事故威脅，並降低可能影響及危害公司運作之損害程度。
2. 本辦法所稱資訊資產係公司所收集、運用、產生之資料，以及為完成上述工作所需使用之相關設備。
3. 人員定義：
   A. 集團員工：泛指集團內部所有定期員工、不定期員工、聘僱人員。
   B. 授權使用者：係指因依業務或職務之需要經程序核定授予管理、操作、存取之權限人員。
   C. 非授權使用者：除授權使用者之外其餘所有人員均為非授權使用者。
4. 管制類別：
   A. 環境:經明確定義並核定為重點管理之特定區域、空間、環境。
   B. 資料:經明確定義並核定為重點管理之特定電磁資料、文件。
   C. 人員:經明確定義並核定為重點管理之特定內、外部人員、組織。
   D. 時間:經明確定義並核定為重點管理之特定時間區段、日期。

陸・作業內容：

一、人員安全評估及管理：

1. 公司對人員之任用及調派，應辦理適當之安全評估與確認其身分背景，考量其職能條件、人格特質、經歷、專業資格能力等。
2. 各部門主管應負責督導所屬員工之資訊作業安全，防範不法及不當行為；對可存取機密性、敏感性資訊或系統者及配賦系統存取特別權限之人員，應妥適分工，分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。

3. 員工自到職日至離職日止。各單位的新進同仁由所屬服務單位向資訊管理單位申請之資源使用權限及帳號，當接受到人員離調申請通知單後 1 個工作天完成帳號調整作業。人員職務調整及調動時，需提出相關證明文件(如離調職單、公告命令等)，再應依系統存取授權規定，限期調整其權限。
4. 公司資訊安全管理辦法應以書面、電子或其他方式告知員工。員工應遵守本辦法所訂定之規範及其他相關資訊安全規定。若違反資訊安全相關規定，得依情節輕重予以處分。
5. 員工應遵守維護業務機密之相關法令規定；在職及離退職後，均不得洩漏所知悉之業務機密或為不當之使用，否則得視其情節輕重予以處分或追究其民、刑事責任。

二、資訊資產安全管理：

1. 全體員工應以之公司資通設備做為公務使用，使用期間不得私自拆卸或蓄意損毀相關零件，並不得私下安裝任何來路不明及非授權軟體，若有軟體安裝需求均需通報資訊單位審查及協助處理。
2. 電腦系統中應安裝防毒軟體或建立防護機制，以防止感染電腦病毒，操作人員並不得任意卸載。
3. USB 或攜帶式儲存設備使用均須填具申請單，經權責單位核准後方可於核准期間開放使用，使用時並應保持警覺切勿隨意存取任何來路不明之檔案。
4. 任何未經授權之非集團內資訊資產設備，嚴禁於廠區內使用以確保資訊安全，各權責主管及資訊管理單位需善盡監督責任，若經查獲將提報懲處並自行負擔任何衍生之法律責任。

三、網路安全管理：

公司網路使用者應遵循以下規定：

1. 不得將自己的登入身份識別帳號與密碼交付他人使用。
2. 不得使用他人的登入身份識別帳號與密碼。
3. 嚴禁下載任何非法及未經授權使用的檔案或軟體，以確保遵循智慧財產權規定。
4. 嚴禁將不當或違反善良風俗習慣之資料於網路上傳送，以維持公司正面形象。
5. 禁止利用公司網路從事不法、不當得利之情事，如有牴觸需自行負擔任何衍生之責任。
6. 全體員工不得以任何手段蓄意干擾或妨害網路系統的正常運作，管理單位有權制止並強制停止其使用權利。
7. 全體員工利用網路公佈及文件交換時，應評估資料安全等級，機密、敏感性，未經當事人同意之個人隱私資料，嚴禁於網路上流通。
8. 機密性或敏感性之資料及文件欲利用電子郵件或其他電子方式傳送時，須以適當的加密或電子簽章等安全技術處理。
9. 外部廠商需經管理單位核可後方可以遠端登入方式進入公司電腦網路系統進行維修，完成後需關閉或停用其存取權限。
10. 未經授權者嚴禁於公司外部網路存取公司內部資源或使用公司相關系統或應用程式，如需 VPN 使用需填具申請單，經核可後方可於核准期限內使用。
11. 如因業務需要須操作特殊連線服務作業，需依正常程序申請核准同意後始得使用。

四．軟體下載之管制：

1. 集團所有廠區禁止使用非法軟體，如有牴觸需自行負擔任何衍生之責任。
2. 經由網路下載軟體，應會同資訊單位事前測試及病毒掃瞄，確認安全無虞後方可安裝及執行。

五・電子郵件之安全管理：

1. 員工如發現來路不明的電子郵件，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞；並應通知電子郵件系統管理者處理。
2. 嚴禁發送電子郵件騷擾他人，導致其他使用者之不安與不便。
3. 嚴禁發送匿名信或偽造他人名義發送電子郵件，詳細內容請參照：2133 電子郵件管理辦法。

六・系統存取管理：

1. 各功能單位對該單位重要之電磁資料應建立機密分級，以落實人員存取管理。
2. 各功能單位應將系統之存取控制需求明確告知系統管理者，以利其執行及維持有效的存取控制機制。
3. 各項正式作業之電腦系統操作及資料處理，由各功能單位指定權責窗口負責建檔、核對、更新、審查及維護電腦資料之正確性。非權責內或未經核准不得操作使用或更改已正式作業之系統檔案。
4. 電腦資料庫及檔案應按不同業務範疇及使用權責區分權限予以保護；重要或具機密性資料在操作或提供使用時，應加強使用者身分之審查，以確保資料安全。

七・資訊作業委外服務之安全管理：

1. 各單位辦理資訊業務委外作業時，有義務及責任通知資訊單位會辦處理，並應於事前明訂廠商之資訊安全責任及保密規定，並列入契約中，要求廠商遵守及考核，並派員監督。
2. 對廠商之軟硬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；基於實際作業需要，得於合約或約定期限內核發臨時性之系統辨識與通行密碼供廠商使用，期限結束後應取消其使用權限。
3. 各單位之重要資料及系統委外廠商處理者，不論在公司內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

八・軟體版權之控管：

全體員工於軟體使用時應嚴格遵守下述規定，如有牴觸需自行負擔任何衍生之責任。

1. 嚴禁員工於工作場所及公司資產內保有或使用未取得授權的軟體。
2. 嚴禁員工在未取得授權同意前，私自將軟體安裝到電腦設備上。
3. 在原授權許可之外的電腦設備上使用軟體時，應取得正式的授權或另行採購。
4. 詳細內容請參照：2012 電腦硬、軟體管理辦法。

九・資料備份：

1. 主機系統應定期執行必要的資料及軟體備份，以便發生災害或時可迅速回復正常作業。
2. 資訊單位應定期檢查及驗證主機備份資料，以確保備份資料之可用性及正確性。
3. 重要資料保存期限應由各功能單位訂定，如有特殊保存需求務必向資訊管理單位提出。

十・電腦媒體使用管理：

1. 應納入管理之電腦媒體包括可攜帶移動的筆記型電腦、PDA、磁帶、磁碟、隨身碟等。
2. 嚴禁攜帶私人儲存周邊裝置及相關儲存媒體。如因職務上或業務上作業產生之需求，皆須依循標準程序申請配給，並於在職其間善盡保管之責，不得有任何違反資訊安全之情事。
3. 各單位保管之媒體儲存的資料，不再繼續使用時，應將儲存的內容消除。

十一・通行密碼之管理：

1. 員工必須負責保護通行密碼，以維持其機密性。
2. 避免將通行密碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。
3. 當有疑似主機系統及使用者密碼可能遭破解時，立即更改通行密碼。
4. 使用者密碼的長度最少應由八位長度組成(不得為空白)。
5. 使用者忘記通行密碼時，需聯絡資訊管理單位協助處理。
6. 使用者必須定期更換通行密碼，原則上以每三個月至少需更新一次；且避免重複或循環使用舊的通行密碼。
7. 使用者登入系統不成功時可以再嘗試的次數，原則上以三次為限。使用者嘗試登入系統連續失敗後將遭系統自動鎖定。

十二・閒置設備之安全管理：

1. 使用者作業結束時，必須完全登出電腦系統或離線。
2. 當電腦設備不使用時，應予以鎖定或其他控管措施保護電腦設備。

十三・資訊設備於外部空間之安全管理：

1. 員工因特殊業務需求於公共場所使用資訊設備時，亦應遵守資訊安全管理授權規定，保持與內部資訊設備相同之安全水準。
2. 電腦設備及資料儲存媒體在公共場所使用時應有專人看管。
3. 筆記型電腦易於遺失或遭未經授權的取用，應提供適當之存取保護措施，如設定通行碼或是將檔案資料加密。

十四・實體與環境之安全管理

1. 為確保電磁資料之保全及資訊資產使用區域之安全，於特別明訂之地點、區域、時間或部門組織，得以加嚴管制之規定以確保機敏資料或重要資訊資產設備之維運。
2. 主機機房及主機備份資料存放地區應嚴格管制人員進出，非經授權之人員不得進入，且須設置門禁管理措施以確保主機安全。
3. 凡經核決程序核定公告之各項管制類別(如:環境、人員、資料、時間)，均應納入特別管制規範，所有相關從業人員均應配合管制規定辦理。

十五・資訊安全事件處理

1. 使用者如偵測到電腦病毒入侵或其他惡意軟體，應立即通知資訊管理人員。
2. 已遭病毒感染的資料及程式應予以隔離或刪除並禁止存取，以避免電腦病毒擴散。
3. 電腦設備如遭病毒感染，應立即離線，直到系統管理人員確認病毒已消除後，才可重新連線。
4. 資訊安全事件區分為:輕度、中度、嚴重等三個等級，各等級應有不同的緊急處置模式:
   A. 輕度:一般性用戶電腦問題或異常網路之活動，無造成資訊環境之影響，由資訊人員處理並排除。
   B. 中度:大規模中毒(超過 10 部資訊資產)或網路癱瘓中斷，已產生資訊環境運作之疑慮，由資訊人員處理並確實記錄事件發生之過程，列入資訊安全紀錄管理。
   C. 嚴重:主機及資料遭內部或外部人員竄改、入侵、控制、盜竊，或發生足以影響集團營運正常活動之資訊安全事件，應由資訊人員會同稽核單位、高階營運主管組成資安事件小組研擬處理對策並詳實紀錄過程，必要時得通報警政單位備案，以保護公司法律層面之權益。

十六・資訊安全事件通報處理機制：

1. 資訊安全事件之通報：

(1) 公司業務如因資訊安全事件致電腦系統無法運作或影響執行效率時，相關人員應視其狀況嚴重程度及影響層面，循序向各權責主管報告。

(2) 集團員工發現有資訊安全事件時，應依公司資訊安全事件通報管道，迅速通報權責主管單位及人員處理。

十七・ 資訊安全之營運持續管理:

1. 集團應明訂資訊安全辦法經核定後公告之，同時應依營運管理變更、法規規範調整、外部趨勢變化等內外部因素適時修訂本辦法以符合管理要求。

2. 為避免資訊資產遭受災害而影響業務永續運作，應訂定應變及復原計畫，並定期測試演練且記錄其過程結果。

3. 企業營運應持續關注外部重大資安議題，資訊權責單位應於外部重大事件發生後二周內完成企業內部風險影響分析報告，並依分析結果三個月內完成具體因應方案，以達風險規避與企業永續之目標。

十八・ 資訊安全之適法性依循:

1. 為確保安全政策必須能夠有效地實施並降低組織違反法律、法規、合約或應盡義務之風險，組織應鑑別所屬產業適用之法條，如:智慧財產權、個人資料保護法、營業秘密保護法、資通安全管理法或其他因業務地區範疇規定之法律，企業組織應善盡管理之責任以力求符合行政法令之規範。

柒、附件：略。