力麒建設股份有限公司

資訊安全管理規範

108 年 12 月 20 日訂立

壹、人員安全管理

一、使用者系統授權

1. 一般標準性使用權限，由權責主管依使用者職務別予以授權。
2. 人員離職時，資料部門人員依「離職申請單」，終止該帳戶。
3. 於系統使用者尚未完成正式授權程序前，資訊服務提供者不得對其提供系統存取服務。
4. 使用者之系統帳號由使用者自訂，不與其他人員衝突為原則，填寫「帳號申請單」經權責主管確認後，交由資訊單位開通。

二、使用者管理

1. 被授權的網路使用者，只可於授權範圍內存取網路資源。
2. 網路使用者不得將自己的登入身份識別帳號與登入網路的密碼交付他人使用。
3. 禁止網路使用者以任何方法竊取他人的登入身份與登入網路通行碼。
4. 禁止網路使用者在網路上取用未經授權的檔案。
5. 網路使用者不得將色情檔案建置在公司網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。
6. 網路使用者不得以任何手段蓄意干擾或妨害網路系統的正常運作。

三、使用者密碼之管理

1. 個人應負責保護通行密碼，維持通行密碼的機密性。
2. 當有跡象足以顯示使用者密碼可能遭破解時，應立即更改密碼。
3. 使用者應盡保密責任，個人密碼不得洩與他人。

貳、電腦主機之安全管理

一、凡由公司提供之電腦設備，各單位須指定專人管理，非經核准不得任意使用、拆卸及更動週邊設備。

二、主機伺服器須設定密碼。

三、嚴禁使用非經授權及來路不明之軟硬體。

四、電腦病毒及惡意軟體之防範

1. 使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。

2. 使用者電腦需安裝防毒軟體。

參、資料安全管理

一、電腦主機資料備份

1. 資料依每日、單週、雙週備份，並作適當歸檔於獨立於電腦主機之外安全處所。

2. 備份人員應將備份媒體異地存放之時間、執行人員及存放事由記載於「備份媒體設備異地進出紀錄」，並定期檢查備份資料之可用性。

二、系統資料回復依據 CC-109 系統復原計畫制度及測試程序之控制作業辦理，資訊單位以最近備份之檔案進行資料回存。

三、電腦開機作業期間，各單位操作員凡發生無法自行排除之故障時，應將發生故障之有關現象記錄下來，洽請資訊單位協助解決。

四、電腦作業環境如溫度、溼度及電源供應之品質等，應隨時監測，如遇特殊需採取必要的補救措施。

五、電腦媒體與資料文件之安全管理。

1. 可重複使用的資料儲存媒體，不再繼續使用時，應將儲存的內容消除。

2. 儲存媒體應依媒體保存規格，存放在安全的環境。

3. 委外處理的電腦文件、設備、媒體蒐集及委外處理資料，應慎選有足夠安全管理能力及經驗的機構作為委辦對象。

4. 應保護重要的資料檔案，以防止遺失、毀壞、被偽造或竄改。

肆、系統安全管理

一、主機系統使用者須設定通行密碼，並須限制使用權限。

二、主機系統須有事件紀錄管理設施，並須每月接受檢查。

三、新系統開發

1. 單位主管初步分析可行時，應指派適任之系統分析人員及相關人員討論作業現況，需求及收集相關資料，確認使用者真正需求.針對系統規格。

2. 新系統開發應先於測試環境確認後，再行上線。

3. 啟用新系統時，應採雙軌制，直到新系統可完全取代舊系統後，方將舊系統淘汰。

四、電腦程式新增或修改

1. 電腦程式之新增，由需求單位提出申請，填寫發出「請購單」經詢、比、議價後，呈權責主管核准。

2. 已完成之程式擬修改時，由使用單位提出需求，評估可行性及成本與效益，經核決權限核准後，委託電腦廠商進行程式修改之工作。

3. 新增及修改之程式應由需求單位進行功能測試，完成無誤後方得進行驗收。

4. 程式新增及修改後，相關之系統文件，使用單位應要求電腦廠商配合提供及修正。

伍、防火牆之安全管理

一、與外界網路連接的網點，應加裝防火牆，以控管外界與公司內部網路之間的資料傳輸與資源存取。

二、若有進入網際網路(Internet)之線路，則需有防火牆(Firewall)管理機制。

三、Internet to Intranet Server 防火牆規則：

1. 定義為公司內伺服器(Intranet Server)對外面 Internet(網際網路)User 提供的網路連線服務規則。

2. 防火牆規則只允許開放給對外網際網路的伺服器(Server) IP Address 與網路連線埠(Port)。

四、Intranet Server to Intranet Server 防火牆規則：

1. 定義為公司內伺服器(Intranet Server)對公司內伺服器(Intranet Server)的網路連線服務規則。

2. 防火牆規則只允許開放公司內有需要相互連線伺服器(Server)的網路連線服務規則，需鎖定 IP Address。

五、Internet Server to Intranet Server 防火牆規則：

1. 定義為公司內伺服器(Intranet Server)對廠商/客戶之伺服器(Internet Server) 的網路連線服務規則。

2. 防火牆規則只允許開放公司伺服器(Server)內有需要與廠商/客戶伺服器(Internet Server)的網路連線服務規則，需鎖定 IP Address 與網路埠(Port)。

六、防火牆建置應設定嚴謹的規則,以防止對外駭客及對內公司員工之有心人士的破壞防，在防火牆規則設定時，應只開放所需服務通行，其餘服務連線皆該禁止通行。

陸、網路服務之安全管理

一、網路設備須有專人管理，隨時監測網路狀況。

二、連外網路須安裝安全防護措施，並須注意可能的系統漏洞。

三、撥接網路須有設定密碼及使用範圍。

四、網路主機應關閉非必要的服務程式。

五、網路系統管理人員應負責製發帳號，供經授權的人員使用。

六、除系統管理者外之系統最高使用權限,應經權責主管人員審慎評估後，交付系統管理者授權並管理。

七、離職人員應取消其存取網路之權利。

八、網路系統管理人員未經權責主管人員許可，不得閱覽、增加、刪除及修改使用者之檔案；但如發現有可疑的網路安全情事，網路系統管理人員得依授權檢查其檔案。

九、網路硬體設備應加裝不斷電系統，以防止不正常的斷電狀況。

十、如果系統使用者為非合法授權的使用者時，網路系統管理人員應立即撤銷其使用者帳號。

十一、對任何網路安全事件，網路系統管理人員應立即向權責主管報告並採取適當應變措施。

柒、系統與網路入侵之處理

一、網路管理者應全面檢討網路安全措施及修正防火牆的設定，以防禦類似的入侵與攻擊。

二、入侵者之行為若觸犯法律規定，構成犯罪事實，應立即通知檢警單位，請其處理入侵者之犯罪事實調查。

捌、設備安全管理

一、設備安置地點之保護

1. 設備應安置在適當的地點並予保護，以減少環境不安全引發的危險及未經授權存取系統的機會。

2. 設備應儘量安置在可減少人員不必要經常進出的工作地點。處理機密性及敏感性資料的工作站，應放置在員工可以注意及照顧的地點。

3. 需要特別保護的設備，應考量與一般的設備區隔，安置在獨立的區域。

二、電源供應

1. 電腦設備之設置，應予保護，以防止斷電或其他電力不正常導致的傷害；電源供應依據製造廠商提供的規格設置。

2. 應考量安置預備電源，並考量使用不斷電系統。

3. 資訊安全事件緊急處理應變計畫應將不斷電系統失效之後的應變措施納入；不斷電系統應依據製造廠商的建議，定期進行測試。

4. 應謹慎使用電源延長線，以免電力無法負荷導致火災等安全情事。

三、設備維護

1. 應妥善地維護設備，以確保設備的完整性及可以持續使用。

2. 應依據廠商合約規範、維修服務期限及說明進行設備維護。

3. 設備的維護只能由授權的維護人員執行。

4. 應將所有的錯誤或是懷疑的錯誤予以記載。

四、設備處理之安全措施

1. 含有儲存媒體的設備項目（例如硬碟）應在處理前詳加檢查，以確保任何機密性、敏感性的資料及有版權的軟體已經被移除。

五、資訊設備誤用之防止

1. 單位員工以及其他第三者，除非獲得正式的授權，任何人皆不得進行職責外系統存取。

玖、周邊安全管理

一、周圍環境之安全

1. 實體環境的安全保護，應以事前劃定的各項周邊設施為基礎，並以設置必要的障礙，達成安全控管的目的。
2. 各項資訊設施之實體保護程度，及實體障礙設置的位置，應依資訊資產及服務系統的價值及安全的風險決定。
3. 周圍設施的安全措施，應視擬保護的資訊資產或資訊服務系統的價值而定。
4. 支援資訊作業的相關設施，應安置在適當的地點，並減少敏感性資訊遭破解及洩漏的機會。
5. 資訊支援人員或維護服務人員，只有在被要求或是被授權的情形下，才能進入限制區域，並視需要限制（例如限制存取敏感性的資料）及監督其活動。
6. 定期向員工宣達資訊安全政策及規定。

二、資訊電腦機房之安全管理

1. 重要業務運作的資訊電腦機房，應設立良好的實體安全措施。
2. 主要的設施應遠離大眾或是公共運輸系統可直接進出的地點。
3. 資訊電腦機房的建築，應儘可能不要有過於明顯的標示。
4. 備援作業用的設備及備援媒體，應存放在安全距離以外的地點，以免資訊電腦機房受到損害時也一併受到毀損。
5. 應安裝適當的安全偵測及防制設備。
6. 機房限制區內應有適當的進出限制保護措施，以確保只有資訊單位人員始得進入，人員進出時應填寫「機房進出紀錄表」及「MIS 機房工作日誌」。

三、辦公桌面之安全管理

1. 文件及儲存媒體在不使用或是不上班時，應存放在櫃內，以避免文件及儲存媒體等在正常的辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

壹拾、電子郵件之安全管理

一、使用者填寫電子郵件帳號之申請經適當核決程序設定啟用，並告知員工使用電子郵件之規定。

二、電子郵件附加之檔案，應事前檢視內容有無錯誤後方可傳送。

三、對來路不明的電子郵件，不宜隨意打開電子郵件或按下郵件內的文字連結，以免啟動惡意執行檔，使網路系統遭到破壞。

四、禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便。

五、禁止網路使用者發送匿名信，或偽造他人名義發送電子郵件。

六、禁止利用電子郵件在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。

七、資訊單位應建立垃圾郵件管理系統，防止垃圾郵件或病毒郵件的攻擊。

壹拾壹、本規範經董事會通過後施行，修正時亦同。