高雄市政府民政局暨所屬機關
資訊安全管理制度

通訊與作業管理程序書

機密等級：內部使用

編　　號：IS-02-008

版本編號：1.3

修訂日期：113.8.5

使用本文件前，如對版本有疑問，請與資安執行小組確認最新版次。

本文件歷次變更紀錄：

版次	發行日	修訂者	說明	核准者
1.0	109 年 7 月 1 日	資安執行小組	初版文件發行	民政局局長
1.1	110 年 12 月 7 日	資安執行小組	修訂部分內容	民政局局長
1.2	111 年 11 月 17 日	資安執行小組	修訂部分內容	民政局局長
1.3	113 年 8 月 5 日	資安執行小組	新增資通安全弱點通報機制(VANS)作業	民政局局長

本文件由資安執行小組負責維護。

目錄

壹、目的

為確保高雄市政府民政局暨所屬兵役處、殯葬管理處、本市各戶政事務所全體機關（以下簡稱本局暨所屬機關）正確安全的操作資訊處理設施及確保網路及其支援之資訊處理設施中資訊之保護，降低各種可能的風險與損害，維護資訊處理與通訊服務之完整性及可用性，特訂定本程序書。

貳、依據

一、本局暨所屬機關資通安全政策。

參、適用範圍

本局暨所屬機關所提供電腦及網路服務之日常管理作業。

肆、權責

一、網路管理人員：規劃及維護網路服務，並執行安全控管機制。

二、系統管理人員：規劃、開發、測試及提供資訊系統服務。

三、權責主管：督導通訊及作業管理，並核准相關作業。

四、網路使用者：在授權範圍內存取網路資源，並遵守通訊及作業安全規範。

伍、名詞解釋

一、 行動裝置：如筆記型電腦、平板電腦及智慧型手機等手持裝置。

二、 可攜式儲存媒體：如磁片、磁碟、磁帶、IC 卡、匣式磁帶、外接式硬碟、光碟、隨身碟、各式記憶卡、錄影帶、錄音帶等便於攜帶使用的電子資料處理或儲存設備。

陸、作業說明

一、 資訊系統安全規劃作業

（一）應建立資訊系統之安全控管機制，以確保資訊資料之安全，保護系統及網路作業，防止未經授權之系統存取。

（二）伺服主機及網路設備應由專責人員負責日常維護，並填寫「系統維護紀錄表」以確保主機能正常運作。

（三）網路管理人員應妥為規劃網路架構、設定網路參數，並依規定備份相關檔案。

（四）有關資訊系統開發、測試與維護作業，請參閱「系統開發與維護程序書」。

（五）有關資訊委外作業，請參閱「委外管理程序書」。

二、容量管理

（一）系統與設備建置前，系統管理人員應適時預估系統容量需求，並對未來容量要求預作規劃，確保有充分處理資料與儲存的空間。

（二）依據日誌儲存需求，配置所需之儲存容量。

（三）應隨時注意及觀察分析系統資源使用情形(如核心資訊系統及網路設備)，監控網路頻寬、CPU、記憶體及儲存空間之使用狀況，找出可能危及系統安全的瓶頸，預作補救措施之規劃，以確保系統與設備可用性。

三、變更管理

（一）系統及資訊處理設施之變更，應建立控制及管理機制。

（二）新增設備及網路變動，應即時修改網路架構圖及「資訊資產清單」。

（三）系統或網路重大變更的事項，應經執行秘書以上核准，並遵循下列規定：

1. 設備之功能性及設定方式應熟悉掌握。
2. 新增對外網路連線，需注意安全性考量，從嚴審核對外網路連線與內部之連接之方式。
3. 如有委外服務供應商參與安裝或設定，應由系統管理人員陪

同並紀錄。

（四）下列變更應填寫「變更申請單」，經權責主管核准後，方可進行變更作業，如遇緊急變更，亦應於變更前口頭向權責主管報告變更需求，權責主管核准後，方可進行變更，且應於變更完成後，進行補單作業：

1. 核心資訊系統之伺服主機、作業系統、資料庫變更，包括：硬體維修、擴充、系統升級、漏洞修補等。
2. 重要網路設備設定變更，包括：防火牆設定變更、核心交換器設定變更。

（五）變更失敗或不能順利執行時，應能回復變更前之狀態。

（六）有關系統變更作業，請參閱「系統開發與維護程序書」。

四、惡意軟體之防範

（一）應安裝病毒偵測軟體，並定期更新病毒資訊（病毒碼），以防止病毒之攻擊，伺服主機防毒軟體系統應設定主動掃瞄檢查。

（二）禁止任意下載或安裝來路不明、有違反法令疑慮（如版權、智慧財產權等）或與業務無關之電腦軟體，亦不得將本局暨所屬機關合法軟體私自拷貝、借予他人或攜回家中使用。

（三）當有跡象顯示可能中毒時，應立即中斷網路連線並儘速通知相關人員，直至確認病毒已消除後，才可重新連線，並填寫「資訊安全事件通報單」留存處理紀錄。

五、電腦軟體與程式著作權保護

（一）應使用授權軟體並遵守著作權規範，違反規範者應依相關程序懲處。

1. 使用軟體與資訊產品不得超過允許的最高使用人數。

2. 使用軟體與資訊產品應遵守相關規定，例如限制於指定之機器使用、限制僅於備份時方可複製等。
3. 取得之合法軟體不得從事或轉讓予非授權範圍之使用。
4. 從公共網路取得之合法軟體與資訊，須遵守原著作權者與個人資料保護法之規定。

（二）採購軟體或於網路下載共享軟體（Shareware）、免費軟體（Freeware）或免費版本的商業軟體，應妥善保管授權書、原版光碟、手冊等資料，並登載於「軟體清冊」，且應進行版本更新作業。

（三）經由網際網路下載之公開授權軟體，應在確認安全無虞及不違反智慧財產權前提下，方得下載使用。

六、網路安全管理

（一）網路服務之管理

1. 避免利用公共網路傳送「密」等級以上資訊，應保護資料在公共網路傳輸之完整性及機密性，並保護連線作業系統之安全性。
2. 網路管理人員應利用網路管理工具，偵測及分析網路流量。
3. 開放相關人員從遠端登入內部網路系統之網路服務，應執行身分辨識作業，或提供連線設備之識別機制。
4. 如發現系統使用者為非合法授權之使用者時，應立即撤銷其系統使用權限。
5. 離（休）職人員應依資訊安全規定及程序，取消其存取網路及系統之權限，並填寫「離職人員帳號停用查核表」。
6. 系統管理人員除依相關法令或規定，不得閱覽使用者之私人

檔案；但如發現有可疑之網路安全情事，系統管理人員得依授權規定，使用工具檢查檔案。

7. 系統管理人員除有緊急狀況外，未經使用者同意，不得新增、或修改私人檔案。

（二）網路使用者之管理

1. 經授權之網路使用者，只能在授權範圍內存取網路資源。
2. 網路使用者應遵守網路安全規定，並確實瞭解其應負之責任；如有違反網路安全情事，應依資訊安全規定，限制或撤銷其網路資源存取權利，並依相關規定處理。
3. 網路使用者不得將自己之登入身分識別與登入網路之通行碼交付他人使用，亦不得以任何方法竊取他人之登入身分與登入網路通行碼。
4. 禁止網路使用者以任何儀器設備或軟體工具竊聽網路上之通訊。
5. 禁止網路使用者在網路上取用未經授權之檔案。
6. 禁止使用本局暨所屬機關網路服務散播色情文字、圖片、影像、聲音等不法或不當之資訊。
7. 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；或以任何手段蓄意干擾或妨害網路系統之正常運作。
8. 禁止任意修改網路相關參數。
9. 為維護本局暨所屬機關網路安全，網路管理人員於發現網路使用者之電腦發送異常封包或使用非經允許之服務時，得中斷其網路使用權限，至改善為止。

（三）防火牆之安全管理

1. 防火牆設定控管由高雄市政府資訊中心統籌辦理，本局暨所屬機關如有自建防火牆，則遵照本程序書辦理。
2. 所有直接與外界網路連接之連線，均應透過加裝防火牆，以控管外界與機房內部網路之間資料傳輸與資源存取。
3. 防火牆應由網路管理人員執行控管設定，並依制定之資訊安全規定、資料安全等級及資源存取之控管策略，建立包含身分辨識機制與系統稽核之安全機制。
4. 防火牆設置完成時，應測試防火牆是否依設定之功能正常及安全地運作。如有缺失，應立即調整系統設定，直到符合既定之安全目標。
5. 網路管理人員應配合資訊安全政策及規定之修正，以及網路設備之變動，隨時檢討及調整防火牆系統設定，調整系統存取權限，以反映最新狀況。
6. 視業務需要及設備功能，對於通過防火牆之特定網路服務，應予確實紀錄。
7. 網路管理人員應避免採取遠端登入方式登入防火牆主機，以避免登入資料遭竊取，危害網路安全。
8. 如必須使用遠端登入，應訂定嚴謹之遠端登入控管措施，並填寫「網路業務處理申請表」。
9. 若資源許可應建立防火牆設備之備援機制；防火牆之環境建置檔等需定期執行備份作業。
10. 網路管理人員定期將防火牆之 log 轉出存放於備份檔案中。
11. 於防火牆設定變更之前，將各防火牆之設定檔備份，相關備

份要求，應遵循本局暨所屬機關「資訊備份管理說明書」要求。

12. 應每年定期清查防火牆規則，刪除或停用閒置（半年以上無觸發紀錄）即已逾申請期限之規則，以確保防火牆規則之適切性。

（四）網路資訊之管理

1. 「內部使用」等級以上之業務資料或文件不得存放於對外開放之資訊系統中，若為執行業務所需，應採取加強之安全管控機制，如通行碼。
2. 網路管理人員應負責監督網路流量及使用情形，並對可能導致系統作業癱瘓等情事，預作有效的防範，以免影響網路服務品質。
3. 對外開放的資訊系統所提供之網路服務，如：HTTP、FTP等，應採取適當之存取控管機制。
4. 網路管理人員於偵測收到資訊系統異常狀況或駭客入侵之警示訊息時，應立即通報權責主管，依據相關作業管理規範採取適當之緊急應變處理，並留存系統異常處理紀錄。

（五）網路入侵之處理

1. 應建立網路入侵事件之調查程序，除利用工具及稽核檔案提供之資料外，應協請相關單位(如網路服務提供者)，追蹤入侵者。
2. 入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知相關單位，請其處理入侵者之犯罪事實調查。
3. 有關資訊安全事件或事故管理，請參閱「安全事件管理程序

書」。

七、電子郵件安全管理

（一）電子信箱帳號之註冊、註銷、異動需向市府資訊中心提出申請，並遵循電子郵件相關管理規範之規定。

（二）應禁止發送匿名信，或偽造他人名義發送電子郵件騷擾他人，導致其他使用者之不安與不便。

（三）「密」等級(含)以上資料或文件，應避免以電子郵件傳送。

（四）不得傳遞大量且非必要的資訊，避免網路壅塞及資源浪費。

（五）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。

（六）對來路不明之電子郵件，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。

八、全球資訊網（WWW）

（一）對 HTTP 伺服器開放可存取的範圍，應限制僅能存取資訊系統之某一特定區域之功能與權限，HTTP 伺服器應透過組態的設定，使其啟動時不具備系統管理者身分。

（二）公告之資訊，應經由權責主管之審查與核定，確認未含機密性或內部使用性的資訊、違反本局暨所屬機關資訊安全管理之相關資訊，以及違反智慧財產權或法令所明定禁止之資訊。

（三）開放外界連線作業之資訊系統，應避免外界直接進入資料庫存取資料。

九、電腦管理及安全防護

（一）所有伺服主機之鐘訊，應單一參考時間源（國家標準時間的時間伺服器）同步。

（二）系統管理人員應定期檢查作業系統及硬體設備之效能，並注意

作業系統版本更新及問題資訊，做適切之因應。

（三）系統管理人員應進行伺服器主機監控，檢查系統、安全及應用程式日誌紀錄、或其它有關之系統狀況。一旦發現任何問題得請相關人員協同處理，必要時並通知委外服務供應商處理。

（四）為提升伺服器主機連線作業之安全性，可視需要使用加密通道（如 VPN、SSH）等各種安全控管技術。

（五）伺服主機應關閉不需要之服務。

（六）系統管理人員應定期檢視更新系統安全修補、防毒軟體及病毒碼，以維持系統正常運作。

（七）軟體由系統管理人員監督安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

十、可攜式儲存媒體管理

（一）系統資料若需以儲存媒體保存時，該媒體應存放於安全設備或處所。

（二）儲存媒體所使用之加密或編碼技術，不應透露予遞送人員或與業務無關之人員。

（三）儲存媒體遞送前應加以妥善包裝保護，避免發生實體損壞。

（四）有關儲存媒體之報廢，請參閱「資訊資產管理程序書」。

十一、資料備份

（一）各項系統設定檔、網頁資料、伺服器檔案及資料庫資料均應由各系統管理人員訂定備份週期，並依據週期執行系統排程或手動備份，相關備份要求請參閱「資訊備份管理說明書」。

（二）重要系統資料應考量建立異地備份機制。

（三）核心系統及網路設備備份資料，應於年度營運持續運作計畫測

試演練時，一併進行還原測試作業，以確保備份資料的可用性。

十二、安全稽核事項

（一）每季應檢視 1 次各設備中系統時間是否一致，並進行校正及同步作業。

（二）系統稽核資料（系統 Log）應依系統重要性進行備份保護作業，並由系統管理者定期檢視，不得新增、刪除或修改稽核資料。

（三）應依據下表進行系統稽核資料保存：

系統/設備名稱	Log 名稱	保存期間需求
核心資訊系統	OS Log	6 個月
	Web Log	6 個月
	AP log	6 個月
	Logon Log	6 個月
	DB Log	6 個月
防火牆	Log	6 個月
核心交換器	Log	6 個月

（四）應定期查核技術符合性，進行弱點掃描或滲透測試，以確定資訊系統及網路環境符合安全實施標準。掃描週期如下：

1. 每年至少針對核心系統之作業系統與網路設備，進行 1 次弱點掃描作業。
2. 新系統上線前應進行滲透測試作業或是原碼檢測作業。

（五）針對技術符合性檢測報告中列為高風險之漏洞應進行修補，並於修補後再次進行檢測，確認該漏洞已經完成修補作業。

（六）應填寫「矯正處理單」，以追蹤高風險漏洞的處理狀態，若高風險漏洞因特定原因，無法進行修補，則應說明緣由，補償性控制措施，並經權責主管核准。

十三、行動裝置管理政策

（一）禁止於即時通訊軟體傳遞「密」及「機密」等資料。

（二）禁止將「密」及「機密」等資料存放於私人行動裝置中。

（三）禁止使用私人行動裝置翻拍本局暨所屬機關「密」及「機密」等資料。

十四、使用者軟體安裝管制

（一）商用軟體安裝與使用，應符合本程序書規範。

（二）免費軟體應於軟體開發商原始網站進行下載使用，若有疑慮，應與本局暨所屬機關資訊人員確認後使用。

（三）共享軟體之使用，須詳細了解其授權規則，若該軟體於試用期滿後須進行採購，則使用者應評估是否採購，或於試用期滿前，將該軟體移除。

十五、資通安全弱點通報機制(VANS)作業

（一）VANS 系統管理員應每個月定期上傳 1 次資訊資產盤點資料，針對高風險以上之弱點，應於一週內至 VANS 系統填寫相關弱點處置方式，並記錄於「資通安全弱點通報機制(VANS)查核清冊」。

（二）VANS 系統管理員每月完成弱點處置後，查核人員應於當月查核資訊資產盤點資料及高風險以上之弱點處理情形。

柒、作業表單

一、IS-04-024 軟體清冊。

二、IS-04-025 網路業務處理申請表。

三、IS-04-026 系統維護紀錄表。

四、IS-04-056 資通安全弱點通報機制(VANS)查核清冊。