南華大學網路安全管理作業規範

105 年 02 月 15 日 104 學年度第 1 次資訊安全暨個人資料保護推行委員會議審議通過
105 年 3 月 28 日 104 學年度第 2 學期第 2 次行政會議審議通過
106 年 05 月 15 日 105 學年度第 1 次資訊安全暨個人資料保護推行委員會議審議通過
106 年 6 月 12 日 105 學年度第 2 學期第 5 次行政會議修訂通過
112 年 06 月 19 日 111 學年度第 1 次資訊安全暨個人資料保護推行委員會議修訂通過
112 年 08 月 14 日 112 學年度第 1 學期第 1 次行政會議修訂通過

一、 南華大學（以下簡稱本校）依據『教育部所屬機關及各級公私立學校資通安全工作事項』制定「南華大學網路安全管理作業規範」（以下簡稱本規範），以維護本校網路使用之安全與保障合法使用之網路流暢度，並建立網路對外服務申辦作業及安全檢查之規範。

二、 本校網路 IP 之管理：

（一）、本校 IP 劃分為四類：實體固定 IP、實體動態 IP、虛擬固定 IP 及虛擬動態 IP;資訊中心依各單位業務需求進行相關配置。

（二）、每單一 IP 或帳號每日流量(即上傳和下載總量)限制為 50GB，計算期間為每日 00:00~23:59，一旦超過流量限制時，該 IP 或帳號頻寬將調降為 5Mbps，直到隔日才能再度恢復正常流量。

（三）、各個單位原則上均採行 DHCP（Dynamic Host Configuration Protocol）方式取得 IP。

（四）、如因教學、研究或行政作業上需求，欲申請固定 IP、網域名稱或需要利用網路進行大量傳輸者，須向本校資訊中心提出申請，經審查核准後始可設定。

（五）、利用本校網路發送非公務信件、入侵他人電腦或干擾網路上其他人之軟硬體系統情節重大者，資訊中心得召開審查小組決定是否停止該帳號使用本校網路之權利。

三、 無線網路之管理：

（一）、為避免干擾無線網路之正常運作及保障本校資訊安全，校內不得私設無線網路基地台；但若因教學、研究或行政作業等需求，得向資訊中心申請核可。

（二）、如需增加無線網路基地台，應向資訊中心申請，經審查核准後始可安裝設定。

四、 防火牆之安全管理：

（一）、內部與外部網路之連接須加裝防火牆，以控管內外網路之連線與

存取。

（二）、防火牆系統之安全控管策略應定期檢討，並作必要之調整。

（三）、防火牆系統軟體，應經常更新版本並定期備份。

（四）、各單位伺服主機或其他具有網路連線功能之設備,若需開放對外連線功能，需向資訊中心申請，經審核通過後始予提供。

（五）、應對網路異常流量進行管理,以提升本校之資訊安全及網路服務品質。

五、 主機安全之防護：

（一）、 開放對外連線之主機，應防制合法使用者身分遭假冒、登入主機進行偷竊、破壞等情事。

（二）、 為提升主機伺服器或其他具有網路連線功能之設備連線作業之安全性，應視需要使用 VPN 等各種安全控管技術，以建立安全及可信賴的通信管道。

（三）、 本校對外提供服務之伺服器，應遵守「南華大學電腦設備安全管理作業規範」。

（四）、 主機應定期進行軟體更新並修補漏洞，資訊中心得協助各單位進行主機安全檢查。

（五）、 禁止使用點對點互連(P2P)軟體或提供分享版權軟體及影音檔案。如因教學、研究或行政作業等需求,得向本資訊中心申請核可。

六、 軟體使用與控制：

（一）、禁止下載、安裝或使用來路不明、未經授權或影響電腦網路環境安全之電腦軟體。

（二）、使用外來檔案，應先進行掃毒，勿任意移除或關閉防毒軟體。若設備中毒導致嚴重影響本校網路,資訊中心得立即停止該設備之網路使用權，並請該設備之管理者進行病毒清除；待設備之管理者向資訊中心回報已完成病毒清除,資訊中心得解除該設備之網路管制。

（三）、各單位採購之軟體，需妥善保存授權證明、原始程式或使用手冊等。

（四）、資訊中心應定期稽核本校公用電腦包括專案電腦、電腦教室、行政電腦等電腦主機，是否有安裝不法軟體。

（五）、網路即時通訊軟體使用原則、規範、安全性需求與購置準則：

1. 本規範所稱即時通訊軟體，指使用者透過網際網路，和特定

對象以語音、文字、影像或檔案進行互動溝通之軟體工具，包含 LINE、臉書 Messenger、ICQ（I Seek You）、Skype、WhatsApp、Telegram、Google Meet、Microsoft Teams 等，與即時通訊系統(遠端桌面)或其他目的及效果相近之軟體。

2. 使用即時通訊軟體傳遞公務訊息，不得涉及機密公務資料或因處理公務上而涉及之個人隱私資訊，並且避免在公共使用電腦登入。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。
3. 使用即時通訊軟體(系統)，裝置應先進行相關之安全環境設定，例如不允許透過手機通訊錄加入好友、關閉「允許利用 ID 加入好友」、阻擋非好友訊息及確認使用之即時通訊軟體（系統）為最新版本等，並且避免在公用電腦登入使用。
4. 通訊群組管理規範：
   （1）由群組管理員負責群組人員之管控，檢查成員正確性，並定期檢視。
   （2）為確保群組內人員之正確性，群組管理員應訂定群組成員命名規則，以識別及確認該成員之正確性，如「單位名稱」、「職稱」及「姓名」。
   （3）發現不明人士要求加入群組時，應予拒絕；例如傳送訊息內容與平時明顯異常有遭冒用之嫌，或已知該帳號被盜用時，應立即封鎖該帳號。
5. 資訊中心若發現即時通訊軟體(系統)異常現象或有危害資訊安全之虞時，得逕行暫停之管制，若經確認為資安事件後，則依「臺灣學術網路各級學校資通安全通報應變作業程序」進行通報。
6. 使用於傳遞公務訊息之即時通訊軟體宜考量下列安全性需求與購置準則：
   (1)用戶端應有身分識別及認證機制。
   (2)訊息於傳輸過程應有安全加密機制。
   (3)伺服器端之主機設備及通訊紀錄應置於我國境內。
   (4)伺服器通訊紀錄（log）應至少保存六個月。

七、 網路使用者違反本規範者依校規及相關獎懲辦法查處。

八、 本校各單位依本規範向資訊中心申請作業時，請填寫本校 ISMS 相關表

單並送交資訊中心；為建立檢核機制，資訊中心應進行適當安全檢核。

九、 本規範經本校資訊安全暨個人資料保護推行委員會及行政會議通過，陳請校長核定後公布實施，修正時亦同。