

# 南華大學105學年度 資訊安全暨個人資料保護推行委員會會議記錄

- 一、會議時間：106年05月15日（星期一）下午3點
- 二、開會地點：成均館三樓會議室(C334)
- 三、出席人員：如簽到記錄
- 四、主 席：吳萬益 學術副校長

紀錄：周容如

## 五、上次會議（105年02月15日）決議事項：

序號	上次會議提案及決議	執行情形
1	提案：新訂「南華大學網路安全管理作業規範」。 決議：照案通過。	已於105年3月28日行政會議提案通過，並已公告於資訊中心網頁。
2	提案：新訂「南華大學電腦設備安全管理作業規範」。 決議：照案通過。	已於105年4月18日行政會議提案通過，並已公告於資訊中心網頁。
3	提案：新訂「南華大學個人資料權利行使作業程序書」。 決議：請資訊中心將名稱修改為「南華大學個人資料權利行使作業程序」，其餘照案通過。	名稱已修改，並已公告於資訊中心網頁。
4	提案：新訂「南華大學個人資料安全保護基本措施」。 決議：照案通過。	已於105年3月7日行政會議提案通過，並已公告於資訊中心網頁。
5	提案：新訂「南華大學個資委外監督履約切結書」與「南華大學委外廠商個資安全維護措施查核表」。 決議：「南華大學個資委外監督履約切結書」與「南華大學委外廠商個資安全維護措施查核表」，照案通過。	1. 已公告於資訊中心網頁。 2. 已請總務處事務組協助針對個資委外廠商填寫切結書及查核表。
6	提案：推動全校進行個資盤點及風險評鑑等工作。 決議：1. 照案通過。 2. 由資訊中心於五月底前統籌協調各單位間於盤點期間所需釐清之疑義。 3. 請研發處研究本校個資保護推動所需經費是否可由獎補款支應。	1. 個人資料保護制度與資訊安全管理規範之建置和驗證委外服務案(案號105-U105000499)已於106年1月13日決標，使用自籌款支應。 2. 相關疑義將由顧問協助解決。

## 七、業務報告事項

- 一、為落實及推動個人資料保護、避免本校因個資外洩導致校譽受損、因應教育部各項評鑑或訪視等要求及符合105年8月5日正式訂定發布之新版「教育體系資通安全暨個人資料管理規範」要求，由資訊中心辦理個人資料保護制度與資訊安全管理規範之建置和通過驗證委外服務案，已於106年1月13日決標。本案分為資訊安全管理及個人資料保護兩部分執行：

### (一) 資訊安全管理

資訊中心於106年2月24日發布新版資通安全管理規範；106年3月20日完成內部稽核；106年4月10日、4月11日完成教育體系資安驗證稽核，稽核結果共開立4項次要缺失(詳如附件一，P4)與12項觀察事項(詳如附件二，P8)。資訊中心於4月21日提出次要缺失之矯正預防措施回覆，目前矯正計畫已通過，已進入發證程序。預計5月底將可取得教育體系資通安全管理規範驗證證書。

### (二) 個人資料保護

#### 1、專案範圍

教務處、學務處、人事室、資訊中心(含以上各處室之二級單位)、產學合作及職涯發展處-職涯及校友服務中心、就學服務處-招生事務組。

#### 2、驗證範圍

教務處-註冊組、學務處-衛生保健組/學生輔導中心/生活輔導組、人事室、資訊中心、產學合作及職涯發展處-職涯及校友服務中心、就學服務處-招生事務組。

#### 3、推動工作項目及時程如附件三(P20)。

- 二、教育部為提高教育體系各學校人員警覺性以降低社交工程攻擊風險，辦理「106年度臺灣學術網路防範惡意電子郵件社交工程演練服務計畫」，(在106年4月~6月進行第1次集中演練,7~9月進行第2次集中演練)，會計算惡意郵件開啟數量，進行點擊率之統計(點閱人數/受測人數)，惡意郵件開啟率應低於10%以下；惡意連結(或檔案)點擊率應低於6%以下，演練成績待改善單位，需提報後續改善計畫，並列為後續教育部資安輔訪對象。

為因應教育部之要求，資訊中心進行宣導事務，包括電子郵件通知、教育訓練(參加人數105人)、協助進行email設定(完成175人數--含自行設定61人、到場協助設定114人)、電話提醒(總數共251人，已完成通知215人)。

## 八、提案討論

### 提案一

**提案單位：**資訊中心

**案由：**修訂「南華大學網路安全管理作業規範」(詳如附件四，P22)，提請討論。

**說明：**1.105 年 03 月 28 日通過之「南華大學網路安全管理作業規範」，經 105 年 06 月 28 日資訊指導委員會委員建議網路異常流量管理機制併入「南華大學網路安全管理作業規範」。

2.修訂對照表詳如附件五(P24)。

**決議：**調整二-5 內容，其餘照案通過。

### 提案二

**提案單位：**管理學院

**案由：**本校教職員離職及學生畢業後之電子郵件帳號是否刪除，提請討論。

**說明：**1.為有效利用系統資源與避免有心人士利用本校管理核發之電子郵件進行違法行為，引發資訊安全或個資保護...等相關之法律問題。

2.提請討論是否於本校教職員離職後及學生畢業後主動刪除其電子郵件。

3.有特殊需求者，可向本校申請繼續使用電子郵件之需求。

**決議：**請資訊中心研究是否可以提供另一個網域之電子郵件給離職教職員及畢業學生使用。新方案確認之前，原則上保留帳號，例外情況刪除。

九、臨時動議：無。

十、散會(16:20)

## 附件四

# 南華大學網路安全管理作業規範(草案)

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

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：

1. 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。
2. 每單一 IP 每日流量(即上傳和下載總量)限制為 10GB，計算期間為每日 00:00~23:59，一旦超過流量限制時，該 IP 當日無法使用網路，直到隔日才能再度使用。
3. 各個單位原則上均採行 DHCP（Dynamic Host Configuration Protocol）方式取得 IP。
4. 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。
5. 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，資訊中心得招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：

1. 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。
2. 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：

1. 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。
2. 防火牆系統之安全控管策略應定期檢討，並作必要之調整。

3. 防火牆系統軟體，應經常更新版本並定期備份。
4. 各單位伺服器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。
5. 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：

1. 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。
2. 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。
3. 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」。
4. 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。
5. 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：

1. 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。
2. 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。**
3. 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。
4. 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。

#### 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。

附件五、修訂對照表

條次	修正後條文	現行條文	說明
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 <b>與保障合法使用之網路流暢度</b> ,並建立網路對外服務申辦作業及安全檢查之規範。	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,並建立網路對外服務申辦作業及安全檢查之規範。	加強文字說明
二-2	<b>每單一 IP 每日流量(即上傳和下載總量)限制為 10GB,計算期間為每日 00:00~23:59,一旦超過流量限制時,該 IP 當日無法使用網路,直到隔日才能再度使用。</b>		增列 IP 每日流量限制與管理說明
二-4	如因教學、研究或行政作業上需求,欲申請固定 IP、網域名稱 <b>或需要利用網路進行大量傳輸者</b> ,須向本校資訊中心 <b>提出</b> 申請,經審查核准後始可設定。	如因教學、研究或行政作業上需求,欲申請固定 IP 或網域名稱,須向本校資訊中心申請,經審查核准後始可設定。	新增網路進行大量傳輸之申請
二-5	<b>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,資訊中心得招開審查小組決定是否停止該帳號使用本校網路之權利。</b>		增列社交攻擊行為之管理事項
六-2	使用外來檔案,應先進行掃毒,勿任意移除或關閉防毒軟體。 <b>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。</b>	如因教學、研究或行政作業上需求,欲申請固定 IP 或網域名稱,須向本校資訊中心申請,經審查核准後始可設定。	新增設備中毒之網路管理事項