



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	1 / 18

管理系統文件

文件類別	第二階文件	
文件編號	IMS-P-002	
文件名稱	資安及個資保護組織管理程序書	
發行單位	國立虎尾科技大學	
發行日期	112年05月05日	
版次	4.3	
適用單位/範圍	全校 (凡業務涉及個資蒐集、處理、利用之單位皆適用之)	
訂修廢單位	審查	核准

(原版簽名頁保存於IMS推動小組)



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	3 / 18

1. 目的

為促使本校有效推動與管理本校「資安及個資保護管理制度(IMS)」，以確保「資安及個資保護管理制度(IMS)」能持續有效地執行，維護本校利害關係人之權益，以提升本校服務水準並且達成既定的資通及個資安全目標。

2. 適用範圍

本校與資安及個資保護組織架構及相關權責之管理。

3. 參考文件

- 3.1 中華民國個人資料保護法。
- 3.2 中華民國個人資料保護法施行細則。
- 3.3 英國國家標準個人資訊管理系統(BS10012：2017)。
- 3.4 國際標準資訊安全管理系統(ISO27001：2013)。
- 3.5 教育體系資通安全暨個人資料管理規範。
- 3.6 IMS-M-003 個人資料保護管理政策。
- 3.7 IMS-P-001 文件與紀錄管理程序書。

4. 名詞定義

4.1 資通安全長(召集人)

組織為確保「資安及個資保護管理制度(IMS)」能有效落實，由校長指派副校長負責監督與管理「資安及個資保護管理制度(IMS)」，以達到預防管理、風險控管及核心業務營運持續之目標。

4.2 業務持續計畫(BCP)

是一套基於業務運行規律的管理要求和規章流程，使組織在面臨突發事件時能夠迅速作出反應，以確保關鍵業務功能可以持續，而不造成業務中斷或業務流程本質的改變。

5. 權責

5.1 資通安全長(召集人)

監督及管理「資安及個資保護管理制度(IMS)」以及督導年度管理審



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	4 / 18

查會議。

5.2 管理審查會議主席

由「資通安全暨個人資料保護推動委員會」召集人擔任，負責主持管理審查會議。

5.3 執行秘書

協助召集人推動及維運「資安及個資保護管理制度(IMS)」，並持續有效地落實各項資安及個資保護管理措施與活動之進行。

5.4 IMS 稽核小組

制定資通安全內部稽核作業管理程序，負責訂定相關之稽核計畫、內部稽核、協助進行外部稽核作業及檢核資通安全業務是否落實。

5.5 IMS 推動小組

報告資安及個資保護資料管理作業之執行狀況。



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	5 / 18

6. 作業內容

6.1 組織與權責管理流程圖

作業流程	權責單位	相關表單
<pre> graph TD A([組織與權責訂修廢]) --> B[相關單位審議] B --> C{核准} C -- 否 --> A C -- 是 --> D[公告或通知] D --> E[組織與權責運作] E --> F{適用性檢討} F -- 適用 --> E F -- 不適用 --> G([紀錄保存]) </pre>	<p>IMS 推動小組</p> <p>相關單位主管</p> <p>資通安全長(召集人)</p> <p>IMS 推動小組</p> <p>相關單位</p> <p>IMS 推動小組</p> <p>IMS 推動小組</p>	<p>資安及個資保護組織架構圖</p> <p>會議紀錄</p> <p>外部單位聯絡清單</p> <p>資通安全暨個人資料保護推動委員會人員名冊</p>



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	6 / 18

6.2 組織與權責訂修廢

6.2.1 資安及個資保護組織架構圖及權責

在「資安及個資保護組織架構圖」中，各項職位之權責，由「IMS 推動小組」負責其訂修廢內容之維護。

6.2.2 各管理程序書之權責

各管理程序書之權責，依照「IMS-P-001 文件與紀錄管理程序書」之規定，由各項業務之主要承辦人員負責其訂修廢內容之維護。

6.3 相關小組審議

6.3.1 「IMS 推動小組」對「資安及個資保護組織架構圖」、各項職位之權責或各管理程序書之權責於訂修廢時，若需相關單位參與討論與審議時，則由「IMS 推動小組」視需要邀集其他相關單位主管進行會議討論。

6.3.2 「IMS 推動小組」遇有權責之爭議無法協調，或牽涉到資安及個資保護組織需進行大變動時，應提交「資通安全暨個人資料保護推動委員會」決議。

6.4 組織與權責核准

「資安及個資保護組織架構圖」、各項職位之權責或各管理程序書之權責之訂修廢內容，應由「IMS 推動小組」之業務承辦人員負責擬案，並依下列規定送呈審核，再依核示意見辦理。

類別 \ 權責	訂、修、廢	審查	核准
資安及個資保護組織架構圖	IMS 推動小組	執行秘書	召集人
各項職位之權責	IMS 推動小組	執行秘書	召集人
各管理程序書之權責	依照「文件與紀錄管理程序書」之規定		

6.5 公告或通知

6.5.1 經核准修正後之「資安及個資保護組織架構圖」應由「IMS 推動小組」負責以適當方式進行公告。

6.5.2 經核准修正後之各項職位之權責、各管理程序書之權責，應由文



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	7 / 18

件管制人員依據「IMS-P-001 文件與紀錄管理程序書」之規定，分發通知相關單位。

6.6 組織與權責運作

「IMS 推動小組」成員在承辦各項業務時，應依照各項職位之權責或各管理程序書之權責規定執行。

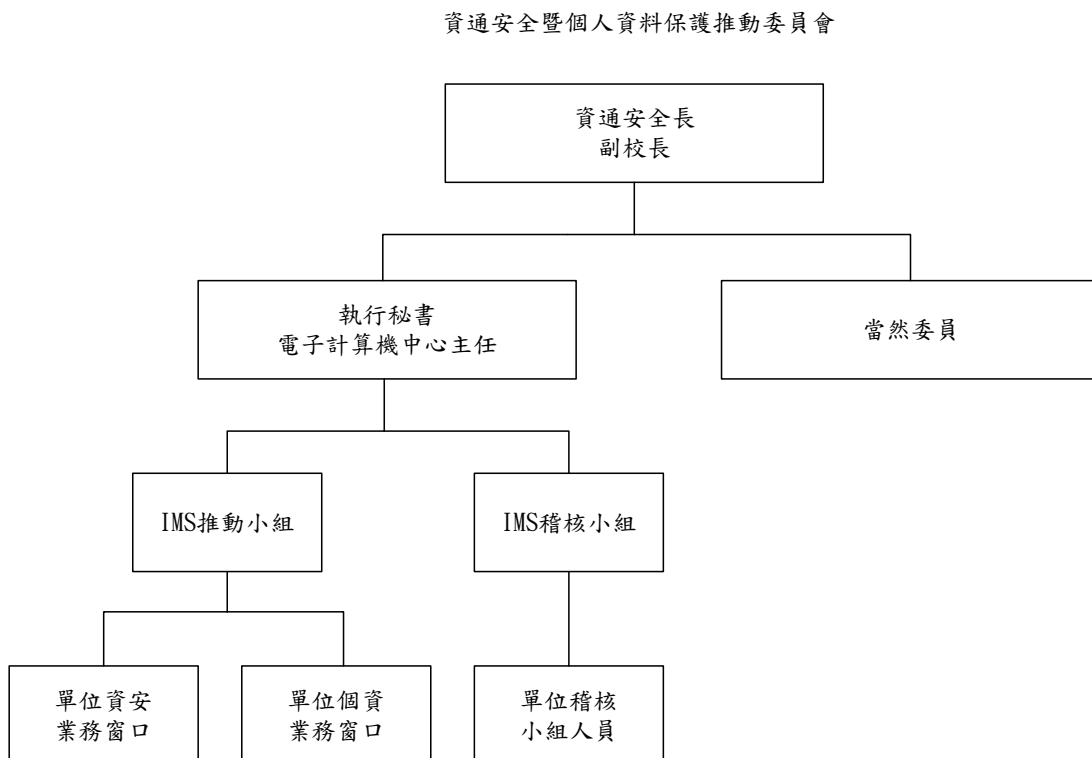
6.7 適用性檢討

「IMS 推動小組」成員在承辦各項業務時，可隨時進行組織與權責適用性之檢討，若有訂修廢之需求時，依照上述之訂修廢規定辦理。

6.8 資安及個資保護管理組織

本校設立「資通安全暨個人資料保護推動委員會」，明確規範資安及個資保護管理作業之人員權限與責任，協調事務及推動資安及個資保護管理事宜，確保資安及個資保護各項管理規範能有效持續地執行，並達成資通及個資安全之政策與目標。本管理組織結構如下。

6.8.1 組織架構圖



6.8.2 組織編組



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	8 / 18

6.8.2.1 資通安全長(召集人)：由校長指派「副校長」擔任負責督導。

6.8.2.2 當然委員：依資通安全暨個人資料保護推動委員會設置要點第四點訂定之，另得由校長另指定委員 1 至 3 人，其任期為 2 年。

6.8.2.3 執行秘書：由電子計算機中心主任擔任，負責四階文件之審核及資安暨個資保護管理制度之推動事宜。

6.8.2.4 IMS 推動小組：統籌各項資安暨個資保護作業原則規劃事宜，由各一級單位為資安保護、以及個資保護分別指派專責人員擔任組成之，電子計算機中心主任指派組長擔任組長。IMS 推動小組組長及分組成員詳見「IMS-P-002-01 資通安全暨個人資料保護推動委員會人員名冊」。

6.8.2.5 IMS 稽核小組：負責資安暨個資保護稽核事宜，由校長指派一位委員擔任組長，各一級單位應派一人參加 IMS 稽核小組，該小組成員必須受過資安暨個資保護稽核訓練。組長及分組成員詳見「IMS-P-002-01 資通安全暨個人資料保護推動委員會人員名冊」。

6.8.2.6 列席人員：視需要指定相關單位人員列席。

6.8.3 資通安全長(召集人)

6.8.3.1 工作職掌

6.8.3.1.1 主持委員會會議對重大事項作出決定或仲裁。

6.8.3.1.2 負責協調相關人員推動「資安及個資保護管理制度(IMS)」。

6.8.3.1.3 審核本校「資安及個資保護管理制度(IMS)」目標及實施範圍。

6.8.3.1.4 「資安及個資保護管理制度(IMS)」執行狀況審查。

6.8.3.1.5 監督營運持續演練的辦理，協調「資安及個資保護管理制度(IMS)」執行所需之相關資源分配。

6.8.3.1.6 審核實施矯正預防措施所需之資源，包括人力、時間及



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	9 / 18

經費。

6.8.3.1.7 負責定期主持管理審查及各項資安與個資保護會議，審查資安及個資保護管理相關事宜。

6.8.4 執行秘書

6.8.4.1 工作職掌

6.8.4.1.1 召集各組成員參加「資安及個資保護管理制度(IMS)」之管理審查及各項資安與個資保護會議。

6.8.4.1.2 向召集人報告「資安及個資保護管理制度(IMS)」管理審查會議結論、執行成果與改善建議事項。

6.8.4.1.3 協調各組監督及執行「資安及個資保護管理制度(IMS)」等各項資安與個資保護工作。

6.8.4.1.4 負責對資安及個資保護狀況進行預警、監控，並對資安及個資保護狀況與事件進行處置。

6.8.4.1.5 對於資安及個資保護管理之改善提出建議，以及協助執行資安與個資保護之自我檢核。

6.8.4.1.6 監督「IMS推動小組」執行「資通安全暨個人資料保護推動委員會」所決議之事項。

6.8.4.1.7 督導資安及個資保護政策之修訂與審核外部評鑑結果。

6.8.4.1.8 每年修訂資安及個資保護量化目標。

6.8.4.1.9 彙總資安及個資保護風險改善建議，於「資通安全暨個人資料保護推動委員會」會議中討論。

6.8.4.1.10 督導定期與不定期風險評估作業之實施。

6.8.4.1.11 資安及個資保護事件處理結果回報資通安全長。

6.8.5 IMS推動小組

6.8.5.1 工作職掌

6.8.5.1.1 「資安及個資保護管理制度(IMS)」文件之發行、回收



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	10 / 18

與銷毀。

- 6.8.5.1.2 「資安及個資保護管理制度(IMS)」文件之版本管理。
- 6.8.5.1.3 發行文件電子檔之保管與發行文件電子文件公告及更新管理。
- 6.8.5.1.4 負責審查「資安及個資保護管理制度(IMS)」文件之初稿，提供改善建議，並將審查完成文件呈核。
- 6.8.5.1.5 負責已核准之「資安及個資保護管理制度(IMS)」文件編碼、發行、保存與控管。
- 6.8.5.1.6 負責「資安及個資保護管理制度(IMS)」各項表單紀錄之彙整。
- 6.8.5.1.7 擬定及辦理資安及個資保護教育訓練計畫與相關活動。
- 6.8.5.1.8 檢討資安及個資保護教育訓練執行成效，並在管理審查會議中提出總結報告。
- 6.8.5.1.9 負責與資安及個資保護相關之宣導與注意事項公告。
- 6.8.5.1.10 每年進行法令法規遵循管理及法規盤點更新作業。
- 6.8.5.1.11 負責建立資安及個資保護事件之預防、應變及復原處理作業。
- 6.8.5.1.12 受理資安及個資保護事件回報與事件處理。
- 6.8.5.1.13 監控、記錄與調查資安及個資保護事件。
- 6.8.5.1.14 建立、演練與維護核心資通系統之業務持續計畫(BCP)。
- 6.8.5.1.15 製作及維護核心資通系統業務持續計畫(BCP)之演練成果報告。
- 6.8.5.1.16 制訂資安及個資保護風險管理制度，每年定期或不定期執行風險評估作業。
- 6.8.5.1.17 持續不斷的評估與檢討風險管理之具體成效。
- 6.8.5.1.18 每年定期或不定期審查風險評估的結果與風險改善處



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	11 / 18

理計畫。

6.8.5.1.19 負責每年定期或不定期資通資產之盤點、彙總、造冊與管理作業。

6.8.5.1.20 負責每年定期或不定期執行「資安及個資保護管理制度(IMS)」驗證範圍內資通資產之風險評估作業。

6.8.5.1.21 負責執行資安及個資保護風險管理作業(包括風險改善計畫、風險改善計畫之後續追蹤與管控)等事宜。

6.8.5.1.22 負責適用性聲明之擬定與傳達。

6.8.5.1.23 參與執行外部評鑑與應對或改善措施。

6.8.5.1.24 每年應向上級或監督機關提出資通安全維護計畫實施情形。

6.8.6 IMS 稽核小組

6.8.6.1 工作職掌

6.8.6.1.1 負責制訂內部稽核作業管理程序。

6.8.6.1.2 負責內部稽核人員之培訓。

6.8.6.1.3 負責制訂及執行內部稽核計畫，協助進行外部驗證稽核作業。

6.8.6.1.4 撰寫稽核總結報告，執行及追蹤稽核缺失之矯正與預防措施之改善，並追蹤缺失事項之執行情形。

6.8.6.1.5 評估與檢討資安及個資保護內部稽核之成效。

6.8.6.1.6 稽查各種安控機制執行狀況並提出稽核總報告。

6.8.6.1.7 在管理審查會議中提出稽核總報告檢討。

6.8.6.1.8 定期或不定期執行全校之資安及個資保護檢查。

6.8.6.1.9 委外廠商契約保密條款及保密切結書之稽核管理。

6.8.7 各單位資安及個資保護專責人員



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	12 / 18

6.8.7.1 成員詳見「IMS-P-002-01 資通安全暨個人資料保護推動委員會人員名冊」。

6.8.7.2 工作職掌

6.8.7.2.1 協助「執行秘書」於各單位執行及運作個人資料管理制度。

6.8.7.2.2 負責管理單位內高風險、敏感及特種個人資料。

6.8.7.2.3 確保所屬單位內或業務內「資安及個資保護管理制度(IMS)」之運作情形及紀錄。

6.8.7.2.4 確保所屬單位或業務資通安全及個人資料保護措施之執行。

6.8.7.2.5 接受對於該單位及業務當事人權利之申請及處理。

6.8.7.2.6 發生個人資料事件單位之聯絡人，應協同「IMS 推動小組」處理個人資料事件。

6.8.8 資通安全專責人員

本校依據「資通安全責任等級分級辦法」設置專責人員，負責本校資通安全各項業務推動。

6.9 資通安全暨個人資料保護推動委員會運作方式

6.9.1 管理審查會議召開

6.9.1.1 每年至少召開管理審查會議一次，由「資通安全暨個人資料保護推動委員會」召集人主持，以確保「資安及個資保護管理制度(IMS)」的適用性和有效性，同時評估改進資安及個資保護管理制度(IMS)。

6.9.1.2 如遇特殊或重大資安及個資保護事件時得召開臨時會議，討論及決議資安及個資保護相關事宜，以因應緊急事故。

6.9.2 管理審查會議參加人員

由「資通安全暨個人資料保護推動委員會」各個成員參加，必要時可邀請學者或與資安及個資保護產業相關的專家與會。



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	13 / 18

6.9.3 管理審查的重點

6.9.3.1 審查各項程序和控制措施的執行成效，主要目標如下：

- 6.9.3.1.1 管理相關程序和控制措施。
- 6.9.3.1.2 快速有效的鑑別資安及個資保護事件。
- 6.9.3.1.3 資安及個資保護活動的實施成效是否符合期望。
- 6.9.3.1.4 反應業務優先順序的資安及個資保護活動。

6.9.3.2 評估「資安及個資保護管理制度(IMS)」執行的有效性，主要目標如下：

- 6.9.3.2.1 執行結果與資安及個資保護政策是否相符。
- 6.9.3.2.2 是否定期更新審查。
- 6.9.3.2.3 是否通報給所有相關人員。
- 6.9.3.2.4 是否確實執行預防與矯正措施。
- 6.9.3.2.5 投入的資源是否足夠。
- 6.9.3.2.6 控制措施是否落實執行。
- 6.9.3.2.7 為查核資通安全控制措施的有效性，各組承辦人員須依據「IMS-P-002-03 ISMS 有效性量測表」之量測項目與量測週期進行評量，並留下紀錄提交管理審查會議審查。

6.9.3.3 分析殘餘和可接受風險，以反應組織、技術、業務目標和流程、鑑別出的威脅以及外部事件(例如法規或社會環境的改變)等事項的改變。

6.9.4 管理審查會議內容

管理審查會議召開前，由「IMS 推動小組」製作「管理審查會議資料」，供會議中進行討論，其資料內容應包括但不限於以下項目：

6.9.4.1 先前管理審查決議事項之跟催狀況。



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	14 / 18

6.9.4.2 有關可能影響 IMS 的外部與內部問題之變更。

6.9.4.3 資安及個資保護的績效回饋，包含下列趨向：

6.9.4.3.1 不符合事項與矯正措施之執行狀況。

6.9.4.3.2 監督與量測結果。

6.9.4.3.3 內部稽核的結果。

6.9.4.3.4 資安及個資保護目標的實現。

6.9.4.4 利害相關團體的回饋。

6.9.4.5 風險評鑑的結果與風險處理計畫的狀態。

6.9.4.6 持續改進的機會。

6.9.4.6.1 訴怨處理。

6.9.4.6.2 已發生的違反/安全事件。

6.9.5 管理審查會議紀錄

管理審查會議由會議主席指派人員負責將會議結果記錄下來，並呈召集人核閱後轉給相關部門傳閱。會議紀錄內容應包括下列事項：

6.9.5.1 IMS 有效性之改進。

6.9.5.2 風險評鑑與風險處理計畫之更新。

6.9.5.3 影響資安及個資保護之程序與控制之必要時的修改，以回應可能衝擊 IMS 之內部或外部事件，包括下列事項之變更：

6.9.5.3.1 各項營運要求。

6.9.5.3.2 各項安全要求。

6.9.5.3.3 影響既有各項營運要求之營運過程。

6.9.5.3.4 法律或法規各項要求。

6.9.5.3.5 契約的各項義務。



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	15 / 18

6.9.5.3.6 風險等級及/或風險接受準則。

6.9.5.4 資源需求。

6.9.5.5 控制措施的有效性如何量測之改進。

6.9.5.6 管理審查為「資安及個資保護管理制度(IMS)」重要之活動，審查會議之紀錄應依「IMS-P-001 文件與紀錄管理程序書」之規定進行控管。

6.9.6 決議事項的跟催

會議決議事項列為下次資安及個資保護內部稽核作業之稽核要項，或由會議中指定專人進行跟催與複查，以確保各項決議事項如期如質地被執行與改善。

6.9.7 會議紀錄陳核

於召開管理審查會議後，由「IMS 推動小組」將會議紀錄彙整並呈報召集人與最高管理階層核閱。

6.10 組織間的合作及協調

本校應與外部單位加強合作協調，實施項目如下：

6.10.1 「IMS 推動小組」應與外部資通專家或顧問加強協調聯繫，以建立相互合作管道，評估本校面臨資安及個資保護威脅之處理措施。

6.10.2 與業務上有密切關係之行政院國家資通安全會報等連結及通信機關，建立及維持適當互動管道，以利發生資安及個資保護危機時，可獲得外部支援解決問題。

6.10.3 由「IMS 推動小組」將與本校「資安及個資保護管理制度(IMS)」相關之資通專家或顧問的聯繫資料紀錄於「IMS-P-002-02 外部單位聯絡清單」中列管，確保於發生資安及個資保護事件時能快速聯繫外單位獲得支援。

6.11 本校就 IMS 推動小組有關內外部之溝通議題鑑別如下：



國立虎尾科技大學

NATIONAL FORMOSA UNIVERSITY

文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	16 / 18

溝通事項	溝通時機	溝通對象	如何溝通
相關法令法規鑑別	每年不定期(至少一次)	政府主管機關	透過網路、公文取得最新版法規
本校資通安全政策、隱私權保護政策、個人資料保護政策	持續溝通	所有利害關係者	透過網站公告本校資通安全政策、隱私權保護政策、個人資料保護政策。
重大資安/個資事件通報	發生重大資安事件時(3、4級)	資通安全長 上級主管機關 行政院國家資通安全會報	透過電話、通訊軟體、資通安全事件報告單、線上填報等方式通報重大資通安全事件。
申訴案件之相關處理,如個資遭到外洩	發生申訴案件時(個資遭到外洩)	當事人、學生、家長或相關利害關係者	透過電話、電子郵件、通訊軟體、書面或親自拜訪等方式,向相關人員進行處置說明,並取得諒解。
採購作業相關事宜與資通安全要求	商品採購時	供應商	依政府採購法辦理。
系統/設備發生故障之相關處理事宜	系統/設備發生故障時	設備維護廠商 專案開發商 委外服務廠商	依照資通業務委外作業管理程序書透過電話、通訊軟體要求維護商進行維修
委外專案相關溝通事宜與資安方面相關要求	委外專案發現Bug、不符需求、或需求變更時	供應商 專案開發商 委外服務廠商	依照資通業務委外作業管理程序書透過電話、電子郵件、通訊軟體、書面等方式向供應商反映



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	17 / 18

本校資通安全與個資防護要求	持續	所有相關利害關係者	透過書面、網站公告 本校資通安全與個資防護相關要求。
資安/個資事件通報	發生資安或個資外洩事件時 (1、2級)	通報至資通安全暨個人資料保護推動委員會執行秘書	透過電話、面報、通訊軟體、資通安全事件報告單等方式通報資通安全事件。
本校有關資安/個資營運、管理、決策	每年定期或系統發生重大變更時	資通安全暨個人資料保護推動委員會	透過管理審查會議溝通有關資安/個資營運、管理、決策等相關內容。
本校之資安政策、個人資料保護、目標、管理程序要求…等。	不定期會議、教育訓練	電子計算機中心 全體員工 校內教職員	外部或內部網站公告 透過教育訓練
管理審查相關輸入事項	每年定期或系統發生重大變更時	資通安全暨個人資料保護推動委員會	會議審查、討論

6.12 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	資通安全暨個人資料保護推動委員會人員名冊	電子計算機中心	至少3年
2	外部單位聯絡清單	電子計算機中心	至少3年
3	ISMS 有效性量測表	電子計算機中心	至少3年

7. 附件

7.1 IMS-P-002-01 資通安全暨個人資料保護推動委員會人員名冊。

7.2 IMS-P-002-02 外部單位聯絡清單。



文件編號	IMS-P-002	文件名稱	資安及個資保護組織管理程序書		
機密等級	內部使用	版次	4.3	頁次	18 / 18

7.3 IMS-P-002-03 ISMS 有效性量測表。