編輯這個表單

教育體系資通安全暨個人資料管理規範(草案第三版) 先期導入自評暨問卷調查

有鑑於新版的《教育體系資通安全暨個人資料管理規範》(以下簡稱：規範草案第三版)，目前規範內容已臻完整，為能瞭解實際施行可改善之處，故希冀藉此問卷獲取貴校/機關寶貴之建議。

規範內容分為以下三部分，請貴校/機關給予指點與建議：

第一部分：
附錄A的第A-71頁至第A-74頁，為針對本次規範草案第三版所「新增適用的控制措施」之羅列與補充說明，此部分的「新增適用控制措施」分為三個層面，共15小題，請貴校/機關就此部分新增的控制措施，自評並提供您的意見。

1.原規範(96年版)刪除之控制措施，於新版規範(105年版)新增：共五小題

2.ISO27001:2013新增或修訂後納入新版規範(105年版)之控制措施：共五小題

3. B級單位「高」等級資訊系統應納入之控制措施：共五小題

第二部分：
請貴校/機關就本規範草案第三版的本文、附錄A、附錄B與資安及個資自評表等文字、內容，提供可改進或修正的意見。

第三部分：
貴校/機關是否願意成為本規範草案先期試行單位，並填寫自評表。

*必填

學校/機關背景調查 *

貴校/機關完成「資訊安全管理制度(ISMS)」驗證情形?(複選)

- [ ] 已通過教版驗證
- [ ] 已通過ISO27001或CNS27001驗證
- [ ] 尚未完成資訊安全管理制度(ISMS)驗證
- [ ] 其他：

若已通過ISO27001或CNS27001驗證者，請於下列空格中寫下是通過何家驗證機構之驗證。

《第一部分》問題一：貴校/單位針對本規範草案第三版附錄A所「新增的控制措施」是否適用? (附錄A 第A-71頁) *

1-1:【原規範為刪除之控制措施】 A.7.1.1 人力資源安全-聘僱之前：篩選「對所有可能被聘用者所進行之背景調查，應依照相關法律、法規及倫理，並應相稱於營運要求及其將存取之資訊保密等級及組織所察覺之風險聘用。」---<<A.7.1.1之實作指引請參第A-8頁與A-9頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

若針對1-1:【原規範為刪除之控制措施】 A.7.1.1 人力資源安全-聘僱之前：篩選，認為 「不符合」或「不適用」，請您於下列空格中寫下原因。

*

1-2:【原規範為刪除之控制措施】A.7.1.2 人力資源安全-聘僱之前：聘用條款及條件 「施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。」---<<A.7.1.2之實作指引請參第A-9頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對1-2:【原規範為刪除之控制措施】A.7.1.2 人力資源安全-聘僱之前：聘用條款及條件 ，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

1-3:【原規範為刪除之控制措施】A.8.3.3 資產管理-媒體處理：實體媒體傳送「應保護含有資訊之媒體在傳送時，不受未經授權的存取、誤用或毀損。」---<<A.8.3.3之實作指引請參第A-14頁與A-15頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對1-3:【原規範為刪除之控制措施】A.8.3.3 資產管理-媒體處理：實體媒體傳送， 認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

1-4:【原規範為刪除之控制措施】A.9.1.1 存取控制-營運要求：存取控制政策「存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。」---<<A.9.1.1之實作指引請參第A-17頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對1-4:【原規範為刪除之控制措施】A.9.1.1 存取控制-營運要求：存取控制政策 ，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

1-5:【原規範為刪除之控制措施】A.9.3.1 存取控制-使用者責任：秘密鑑別資訊之使用「於使用秘密鑑別資訊時，應要求使用者遵循施行單位之實務規定。」----<<A.9.3.1之實作指引請參第A-20頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對1-5:【原規範為刪除之控制措施】A.9.3.1 存取控制-使用者責任：秘密鑑別資訊之使用 ，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

《第一部分》問題二：貴校/單位針對本規範草案第三版附錄A所「新增的控制措施」是否適用?(附錄A第-72頁) *

2-1:【ISO27001:2013新增或修訂後納入之控制措施】A.14.2.5 系統獲取開發及維護：保全系統工程原則「保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。」---<<A.14.2.5之實作指引請參第A-46頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對2-1:【ISO27001:2013新增或修訂後納入之控制措施】A.14.2.5 系統獲取開發及維護：保全系統工程原則，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

2-2:【ISO27001:2013新增或修訂後納入之控制措施】A.15.1.1 供應者關係：供應者關係之資訊安全政策「應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。」---<<A.15.1.1之實作指引請參第A-49頁與A-50頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對2-2:【ISO27001:2013新增或修訂後納入之控制措施】A.15.1.1 供應者關係：供應者關係之資訊安全政策 ，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

2-3:【ISO27001:2013新增或修訂後納入之控制措施】A.16.1.4 資訊安全事故管理：資訊安全事件評估及政策「應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。」---<<A.16.1.4之實作指引請參第A-53頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對2-3:【ISO27001:2013新增或修訂後納入之控制措施】A.16.1.4 資訊安全事故管理：資訊安全事件評估及政策，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

2-4:【ISO27001:2013新增或修訂後納入之控制措施」A.16.1.5資訊安全事故管理：對資訊安全事故之回應 「應依文件化程序，回應資訊安全事故。」---<<A.16.1.5之實作指引請參第A-53頁與A-54頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對2-4:【ISO27001:2013新增或修訂後納入之控制措施」A.16.1.5資訊安全事故管理：對資訊安全事故之回應，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

2-5:【ISO27001:2013新增或修訂後納入之控制措施】A.17.2.1 營運持續管理之資訊安全面：資訊設備之可用性 「應對資訊處理設施實作充分之多重備援，以符合可用性要求。」---<<A.17.2.1之實作指引請參第A-57頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對2-5:【ISO27001:2013新增或修訂後納入之控制措施】A.17.2.1 營運持續管理之資訊安全面：資訊設備之可用性，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

《第一部分》問題三：貴校/單位針對本規範草案第三版附錄A所「新增的控制措施」是否適用?(附錄A第A-73頁與A-74頁) *

3-1:【B級單位「高」等級資訊系統應納入之控制措施】A.14.1.3 系統獲取開發及維護：保護應用服務交易 「應保護應用服務交易中涉及之資訊，以防止不完整的傳輸、誤選路(mis-routing)，未經授權之訊息修改、未經授權之揭漏、未經授權之訊息複製或重演。」---<< A.14.1.3之實作指引請參第A-44>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對3-1:【B級單位「高」等級資訊系統應納入之控制措施】A.14.1.3 系統獲取開發及維護：保護應用服務交易 ，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

3-2:【B級單位「高」等級資訊系統應納入之控制措施】A.14.2.1 系統獲取開發及維護：保全開發政策 「應建立軟體及系統開發之規則，並應用至施行單位內之開發。」---<<A.14.2.1之實作指引請參第A-44頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對3-2:【B級單位「高」等級資訊系統應納入之控制措施】A.14.2.1 系統獲取開發及維護：保全開發政策 ，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

3-3:【B級單位「高」等級資訊系統應納入之控制措施】A.14.2.6 系統獲取開發及維護：保全開發環境 「對涵蓋整個系統開發生命週期之系統開發及整合工作，施行單位應建立並適切地保護安全開發環境。」---<<A.14.2.6之實作指引請參第A-46頁與A-47頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對3-3:【B級單位「高」等級資訊系統應納入之控制措施】A.14.2.6 系統獲取開發及維護：保全開發環境 ，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

3-4:【B級單位「高」等級資訊系統應納入之控制措施】 A.14.2.8 系統獲取開發及維護：系統安全測試 「於開發中，應實施安全功能之測試」---<<A.14.2.8之實作指引請參第A-47頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對3-4:【B級單位「高」等級資訊系統應納入之控制措施】 A.14.2.8 系統獲取開發及維護：系統安全測試，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

*

3-5:【B級單位「高」等級資訊系統應納入之控制措施】A.15.1.3 供應者關係：資訊及通訊技術供應鏈 「與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。」---<<A.15.1.3之實作指引請參第A-50頁>>

- [ ] 符合
- [ ] 不符合
- [ ] 不適用

針對3-5:【B級單位「高」等級資訊系統應納入之控制措施】A.15.1.3 供應者關係：資訊及通訊技術供應鏈，認為「不符合」或「不適用」，在請您於下列空格中寫下原因。

《第二部分》請貴校/機關就本規範草案第三版的本文、附錄A、附錄B與資安及個資自評表等文字、內容，提供可改進或修正的意見。

若對於本規範草案第三版中的文字與內容說明有不明瞭或可改進、修正之部分，請不吝給予指教，留下您寶貴的意見。

《第三部分》貴校/機關是否願意成為本規範草案先期試行單位，並填寫自評

表。 *

因目前規範草案已屆第三版之階段，內容業已大致成熟、完整，但仍有許多細節之處係待實際施行始能發覺，故在此詢問貴學校/機關，是否願意成為我們第一階段試行單位，有無意願都請您留下建議，我們將把您的意見轉呈給教育部資科司。

- [ ] 若有經費補助則願意
- [ ] 無經費補助仍願意
- [ ] 無論有無經費補助皆不願意

*

貴校/機關是否有規劃導入新版教版資安/個資驗證?(複選) *

- [ ] 有意願導入新版教版資安驗證
- [ ] 有意願導入教版個資驗證

感謝您的作答，我們將會把您的意見納入參考，謝謝您! *

請留下貴校/機關名稱

*

請留下填卷人之姓名

*

請留下填卷人的任職單位/部門及職稱

*

請留下填卷人的電子信箱

個人資料提供同意書

1.教育機構資安驗證中心(下簡稱本中心)向您蒐集之個人資料，目的在於瞭解各學校/機關對於規範草案之想法，並徵求有意願成為第一階段試行單位，進而蒐集、處理及使用您的個人資料，但上述行為皆受個人資料保護法及相關法令之規範。

2.本次蒐集之個人資料如問卷內文所列，包含姓名、學校/機構名稱、部門、職稱與電子信箱等得以直接或間接識別個人之相關資訊。期限自取得起始日至特定目的的終止日為止，並遵守個人資料保護法之規定妥善保護您的個人資訊。

3.您同意本中心因規範草案修改以及徵詢試辦學校/機關所需，以您所提供的個人資料確認您的身份、與您進行聯絡。

4.本同意書如有未盡事宜，依個人資料保護法或其他相關法規之規定辦理。

5.您瞭解此一同意書符合個人資料保護法及相關法規之要求，並具有書面同意本中心蒐集、處理及使用您的個人資料之效果。

*

○ 我已詳閱本同意書，瞭解並同意受同意書之拘束（請勾選）。

提交

請勿利用 *Google* 表單送出密碼。

100%：恭喜完成！