景 文 科 技 大 學

個資暨資安業務委外監督管理作業說明書

本文件為管制性文件，任何人非經核准不得複製或對外發行

機密等級：■一般 □限閱 □敏感 □機密

版　　本：1.4
文件編號：PIMS-3-02
生效日期：2025/07/17
製作人員：謝秉成
總 頁 數：12

目　　錄

0 修改記錄

版本	生效日期	修改記錄	修改人
1.0	2015/06/01	初版發行	簡采羚
1.1	2016/11/29	文字酌作調整 原文： 6.2.3 委外廠商服務內容變更的管理規定，會與~~各~~別委外廠商於契約書中載明，如委外廠商人員變更時，須來文經主辦單位同意後，始得變更。 修改： 6.2.3 委外廠商服務內容變更的管理規定，會與**個**別委外廠商於契約書中載明，如委外廠商人員變更時，須來文經主辦單位同意後，始得變更。 文字酌作調整 原文： 6.5 服務變更：合約內容或標的物如有變更，應重新檢視修訂安全條款避免產生安全~~暇~~隙。 修改： 6.5 服務變更：合約內容或標的物如有變更，應重新檢視修訂安全條款避免產生安全**瑕**隙。 編碼方式修改 原文： 7 附件 7.1 委外廠商保密切結書（~~FO~~-PIMS-3-02-01） 7.2 委外廠商作業涉及個人資料安全維護檢核表（~~FO~~-PIMS-3-02-02） 修改： 7 附件 7.1 委外廠商保密切結書（**PIMS-3-02-01**） 7.2 委外廠商作業涉及個人資料安全維護檢核表（**PIMS-3-02-02**）	簡采羚
1.2	2022/07/19	年度檢視調整文字符合現況 原文： 3 適用範圍 ~~本說明書適用於本校因應內部或提供當事人相關服務涉及業務委外活動，均屬於本說明書之適用範圍。~~ 修改： 3 適用範圍 **本校因業務需求委外辦理之個資或資訊業務活動，均屬本說明書適用範圍。** 原文：	謝秉成

		6.2.1 主辦單位應視委外作業涉及個人資料之敏感程度要求得標廠商，定期（如，期中或期末）針對相關之個人資料安全維護情形以會議或書面的方式進行報告或填寫「委外廠商作業涉及個人資料安全維護檢核表」，主辦單位得對於有疑慮之項目進行實地之查核，以證明善盡監督之責任。 修改： 6.2.1 主辦單位應視委外作業涉及個人資料**或資訊安全**之敏感程度要求得標廠商，定期（如，期中或期末）針對相關之個人資料**或資訊**安全維護情形以會議或書面的方式進行報告或填寫「委外廠商作業涉及個人資料**暨資訊**安全維護檢核表」，主辦單位得對於有疑慮之項目進行實地之查核，以證明善盡監督之責任。 原文： 6.2.2 受委託廠商若有得分包或轉包之情形，應先取得主辦單位之書面同意後始可為之，並交付「複委託之契約副本」、「委外廠商保密切結書」與「委外廠商作業涉及個人資料安全維護檢核表」。 修改： 6.2.2 受委託廠商若有得分包或轉包之情形，應先取得主辦單位之書面同意後始可為之，並交付「複委託之契約副本」、「委外廠商保密切結書」與「委外廠商作業涉及個人資料**暨資訊**安全維護檢核表」。 原文： 6.3.1 受委託廠商應於履約結束後，提交專案期間受委託之個人資料相關保護情形，並列於驗收的項目中。 修改： 6.3.1 受委託廠商應於履約結束後，提交專案期間受委託之個人資料**或資訊業務**相關保護情形，並列於驗收的項目中。 原文： 7.2 委外廠商作業涉及個人資料安全維護檢核表（PIMS-3-02-02） 修改： 7.2 委外廠商作業涉及個人資料**暨資訊**安全維護檢核表（PIMS-3-02-02）	

1.3	2024/7/23	因應 ISO 27001 改版進行修訂 新增： … 7　雲端服務安全管理 7.1 使用雲端服務類型 7.1.1　基礎設施即服務(IaaS)：使用者可挑選使用到的網路、儲存容量、伺服器進行付費，不須支出維護與購買硬體的費用。例如：Amazon EC2。 7.1.2　平臺即服務(PaaS)：除 IaaS 的服務項目外，使用者還可以開發、測試、管理及建置自己的應用程式。例如：Google App Engine。 7.1.3　軟體即服務(SaaS)：除 IaaS 加 PaaS 的服務項目外，可以透過網路或瀏覽器進入雲端作業系統在電腦上使用雲端的應用程式，無須購買或安裝軟體在硬體設備上。例如：Microsoft Office365、Outlook。 7.2 使用雲端服務前雲端服務供應商之評估 使用雲端服務前宜了解雲端服務商的資訊安全能力，雙方之共同責任的分野，至為重要： 7.2.1　評估使用雲端服務相關聯的服務範圍，及需那些資訊安全要求事項，定義資訊安全控制措施中那些須本校自行管理(如資料備份)，那些由雲端服務供應商提供。如本校使用雲端服務中有檔案存取，至少須有防火牆(含 IPS)、網頁(Email)過濾、網路安全監控、防毒等防護要求。 7.2.2　評估雲端服務供應商提供之資訊安全能力與資訊安全控制措施的保證，做為選擇使用雲端服務等級的依據。 7.2.3　評估了解雲端服務供應商處理或儲存資訊之地理位置，及不同管轄權之數位證據法律及法規。 7.2.4　定義本校使用雲端服務管理者。 7.2.5　不選取雲端服務有進一步分包予外部供應者的供應商。 7.2.6　上述評估填寫「使用雲端服務評估表」，並經主管核可。 7.3 使用雲端服務之管理 本校為確保使用雲端服務之資料之機密性、完整性、可用性需進行如下管理： 7.3.1　使用雲端服務之存取控制依據 「ISMS-02-008_系統與網路安全管理程序書」之帳號管理、通行碼（密碼）之使用、系統維護帳號及系統特許權限帳號管理、Email 管理原則。 7.3.2　資料上傳與下載均應先行使用掃毒程式掃描。 7.3.3　提供雲端外部存取服務時，須考慮外部作業	謝秉成

		的安全性，至少應確保遠端的存取、處理及儲存的機密性與安全性，如建立白名單與 VPN 的機制。 7.3.4　網路管理者的責任依據「ISMS-02-008_系統與網路安全管理程序書」之網路管理定期進行一般帳號與特權帳號盤查。 7.3.5　使用雲端服務環境中發生資訊安全事件時，需依據「ISMS-02-011_資訊安全事件管理程序書」之規範進行資訊安全事件之通報、事件排除及回復等作業。 7.3.6　使用雲端服務中有安裝本校自行開發系統軟體，於上架(含系統改版)前須做源碼檢測，並至少須無中高以上弱點風險才可上架。參閱「ISMS-02-010_資訊系統獲取、開發及維護管理程序書」之規範進行系統軟體資訊安全控管。 7.3.7　使用雲端服務中的資料備份，需依據「ISMS-03-008_資料備份作業指導書」之規範進行資料備份及定期進行資料回復持續演練。 7.3.8　使用雲端服務中之應用套裝軟體，如 Office365、mail、瀏覽器之組態，需依據相關規範進行管理。 7.4 停止雲端服務之管理 如本校欲停止使用雲端服務，須防護確保資料之機密性、完整性及可用性，確保無外洩或遺失之虞，需進行如下管理： 7.4.1　停止使用前，在雲端資料須做一完整備份，如 Email 檔案、一般資料檔案、組態檔案及原始碼(如有)。 7.4.2　須將雲端資料刪除，如應用程式、一般資料檔案等，並填寫「資料銷毀計畫表」，經主管核可。 相關表單新增： 使用雲端服務評估表(PIMS-3-02-03)	
1.4	2025/7/17	因應資安專章委化資安強化推動策略，新增委外廠資通安全查核項目表，並修正個人資料檢核表回原來名稱-委外廠商作業涉及個人資料安全維護檢核表，分兩表，視委外系統狀況使用之。 原文: 6.2.1　主辦單位應視委外作業涉及個人資料或資訊安全之敏感程度要求得標廠商，定期（如，期中或期末）針對相關之個人資料或資訊安全維護情形以會議或書面的方式進行報告或填寫「委外廠商作業涉及個人資料暨資訊安全維護檢核表」，主辦單位得對於有疑慮之項目進行實地之查核，以證明善盡監督之責	

		任。 修改: 6.2.1　主辦單位應視委外作業涉及個人資料或資訊安全之敏感程度要求得標廠商，定期（如，期中或期末）針對相關之個人資料或資**通**安全維護情形以會議或書面的方式進行報告或填寫「**委外廠商作業涉及個人資料安全維護檢核表**」或「**委外廠商資通安全查核項目表**」，主辦單位得對於有疑慮之項目進行實地之查核，以證明善盡監督之責任。 原文: 6.2.2　受委託廠商若有得分包或轉包之情形，應先取得主辦單位之書面同意後始可為之，並交付「複委託之契約副本」、「委外廠商保密切結書」與「委外廠商作業涉及個人資料暨資訊安全維護檢核表」。 修改: 6.2.2　受委託廠商若有得分包或轉包之情形，應先取得主辦單位之書面同意後始可為之，並交付「複委託之契約副本」、「委外廠商保密切結書」與「**委外廠商作業涉及個人資料安全維護檢核表**」或「**委外廠商資通安全查核項目表**」。 相關表單 原文: 8.2 委外廠商作業涉及個人資料暨資訊安全維護檢核表（PIMS-3-02-02） 修改: 8.2 **委外廠商作業涉及個人資料安全維護檢核表（委外廠商資通安全查核項目表**(PIMS-3-02-02) 新增： 8.4 委外廠商資通安全查核項目表(PIMS-3-02-04)	

1 目的

景文科技大學（以下簡稱本校）為確保委外作業之安全，特訂定「個資暨資安業務委外監督管理作業說明書」(以下簡稱本說明書)。

2 依據

2.1 個人資料保護法

2.2 個人資料保護法施行細則

2.3 本校個人資料保護政策

2.4 本校資訊安全政策

2.5 本校個人資料保護管理執行小組設置要點

3 適用範圍

本校因業務需求委外辦理之個資或資訊業務活動，均屬本說明書適用範圍。

4 名詞解釋

請查閱「個人資料文件名詞解釋彙整表」。

5 權責

5.1 依本校「個人資料保護推行組織與責任分工程序書」6、組織職責辦理。

5.2 依本校「資訊安全組織程序書」4、組織與分工辦理。

6 作業說明

6.1 委外招標階段

6.1.1 主辦單位應審慎評估可能的潛在安全風險，依不同服務，將個資與資訊安全責任及保密規定列入服務契約，要求委外廠商遵守。

6.1.2 委外廠商及人員，均需簽署其安全角色與責任的協議，如「委外廠商保密切結書」供得標廠商於得標後交付使用。

6.1.3 進行委外廠商及人員資格審查。

6.2 委外履約階段

6.2.1 主辦單位應視委外作業涉及個人資料或資訊安全之敏感程度要求得標廠商，定期（如，期中或期末）針對相關之個人資料或資訊安全維護情形以會議或書面的方式進行報告或填寫「委外廠商作業涉及個人資料安全維護檢核表」或「委外廠商資通安全查核項目表」，主辦單位得對於有疑慮之項目進行實地之查核，以證明善盡監督之責任。

6.2.2 受委託廠商若有得分包或轉包之情形，應先取得主辦單位之書面同意後始可為之，並交付「複委託之契約副本」、「委外廠商保密切結書」與「委外廠商作業涉及個人資料安全維護檢核表」或「委外廠商資通安全查核項目表」。

6.2.3 委外廠商服務內容變更的管理規定，會與個別委外廠商於契約書中載明，如委外廠商人員變更時，須來文經主辦單位同意後，始得變更。

6.3 委外契約履約完成

6.3.1 受委託廠商應於履約結束後，提交專案期間受委託之個人資料或資訊業務相關保護情形，並列於驗收的項目中。

6.3.2 除非相關法律有特別之規定，受委託廠商應於履約完成後進行個人資料載體之返還，以儲存方式而持有之個人資料需安全的刪除，並提供確切之證據，主辦單位得對於有疑慮之項目進行實地之查核。

6.4 委外廠商安全管理

6.4.1 委外廠商與作業人員應遵守本校個資安全管理制度及資訊安全管理制度之規定。

6.4.2 安全認知：委外廠商作業人員到點服務除需依規定簽署委外廠商保密切結書外，主辦單位應告知作業項目及場所相關安全管理規定。

6.4.3 委外廠商應提供資安與個資安全事故或事件通報之適當管道。

6.4.4 委外廠商場所安全：

6.4.4.1 主辦單位應依個資之機敏等級，於合約中適度要求委外廠商確保該作業場所安全，如實體環境的安全周界、人員出入門禁管理、外部環境威脅及員工應在安全區域內工作等安全事項。

6.4.4.2 主辦單位宜不定期前往該委外廠商視查個資安全保護狀況,並可視狀況要求該廠商改進,以防止個資外洩事故或其他違法情事之發生。

6.4.5 委外廠商電腦設備安全：

6.4.5.1 主辦單位應要求委外廠商應對資訊等電腦設備進行必要之保護及保密措施，以防止設備、個人資料之遺失、竊盜及損毀的事故發生。

6.4.5.2 主辦單位應要求委外廠商對於個資處理或管理之人員帳號及密碼管理等，應有完善的管制措施。

6.4.5.3 主辦單位應要求委外廠商對離職人員所參與之作業,進行帳號清查、密碼變更及相關資訊資產繳回事宜。

6.5 服務變更：合約內容或標的物如有變更，應重新檢視修訂安全條款避免產生安全瑕隙。

7 雲端服務安全管理

7.1 使用雲端服務類型

7.1.1 基礎設施即服務(IaaS)：使用者可挑選使用到的網路、儲存容量、伺服器進行付費，不須支出維護與購買硬體的費用。例如：Amazon EC2。

7.1.2 平臺即服務(PaaS)：除 IaaS 的服務項目外，使用者還可以開發、測試、管理及建置自己的應用程式。例如：Google App Engine。

7.1.3 軟體即服務(SaaS)：除 IaaS 加 PaaS 的服務項目外，可以透過網路或瀏覽器進入雲端作業系統在電腦上使用雲端的應用程式，無須購買或安裝軟體在硬體設備上。例如：Microsoft Office365、Outlook。

7.2 使用雲端服務前雲端服務供應商之評估

使用雲端服務前宜了解雲端服務商的資訊安全能力，雙方之共同責任的分野，至為重要：

7.2.1 評估使用雲端服務相關聯的服務範圍，及需那些資訊安全要求事項，定義資訊安全控制措施中那些須本校自行管理(如資料備份)，那些由雲端服務供應商提供。如本校使用雲端服務中有檔案存取，至少

須有防火牆(含 IPS)、網頁(Email)過濾、網路安全監控、防毒等防護要求。

7.2.2 評估雲端服務供應商提供之資訊安全能力與資訊安全控制措施的保證，做為選擇使用雲端服務等級的依據。

7.2.3 評估了解雲端服務供應商處理或儲存資訊之地理位置，及不同管轄權之數位證據法律及法規。

7.2.4 定義本校使用雲端服務管理者。

7.2.5 不選取雲端服務有進一步分包予外部供應者的供應商。

7.2.6 上述評估填寫「使用雲端服務評估表」，並經主管核可。

7.3 使用雲端服務之管理

本校為確保使用雲端服務之資料之機密性、完整性、可用性需進行如下管理：

7.3.1 使用雲端服務之存取控制依據「ISMS-02-008_系統與網路安全管理程序書」之帳號管理、通行碼（密碼）之使用、系統維護帳號及系統特許權限帳號管理、Email 管理原則。

7.3.2 資料上傳與下載均應先行使用掃毒程式掃描。

7.3.3 提供雲端外部存取服務時，須考慮外部作業的安全性，至少應確保遠端的存取、處理及儲存的機密性與安全性，如建立白名單與 VPN 的機制。

7.3.4 網路管理者的責任依據「ISMS-02-008_系統與網路安全管理程序書」之網路管理定期進行一般帳號與特權帳號盤查。

7.3.5 使用雲端服務環境中發生資訊安全事件時，需依據「ISMS-02-011_資訊安全事件管理程序書」之規範進行資訊安全事件之通報、事件排除及回復等作業。

7.3.6 使用雲端服務中有安裝本校自行開發系統軟體,於上架(含系統改版)前須做源碼檢測，並至少須無中高以上弱點風險才可上架。參閱「ISMS-02-010_資訊系統獲取、開發及維護管理程序書」之規範進行系統軟體資訊安全控管。

7.3.7 使用雲端服務中的資料備份，需依據「ISMS-03-008_資料備份作業指導書」之規範進行資料備份及定期進行資料回復持續演練。

7.3.8 使用雲端服務中之應用套裝軟體，如 Office365、mail、瀏覽器之組態，需依據相關規範進行管理。

7.4 停止雲端服務之管理

如本校欲停止使用雲端服務，須防護確保資料之機密性、完整性及可用性，確保無外洩或遺失之虞，需進行如下管理：

7.4.1 停止使用前，在雲端資料須做一完整備份，如 Email 檔案、一般資料檔案、組態檔案及原始碼(如有)。

7.4.2 須將雲端資料刪除，如應用程式、一般資料檔案等，並填寫「資料銷毀計畫表」，經主管核可。

8 附件

8.1 委外廠商保密切結書（PIMS-3-02-01）

8.2 委外廠商作業涉及個人資料安全維護檢核表（PIMS-3-02-02）

8.3 使用雲端服務評估表(PIMS-3-02-03)

8.4 委外廠商資通安全查核項目表 (PIMS-3-02-04)