

		義守大學 ISO-27001 資訊安全管理系統			
文件 名稱	資訊安全政策	文件編號	P9-01	制/修訂日	2024.06.25
		版次	第 2.2 版	頁次	1/7

1. 目的：

本安全政策係以本校之核心業務為主，並依據 ISO-27001/CNS-27001 為標準作為發展本校資通安全管理制度之承諾。為達到資通安全之管理需求，依據本安全政策規劃及推動資通安全管理制度，並視實施成效做為進一步擴展之參考。冀望資通安全管理制度之實施，可促使本校各項電子化作業之設計開發、使用管理及營運維護等工作的安全性，以及保障本校資訊之機密性、完整性、可用性及遵循性。

2. 政策：每年由本校於「ISO-27001 年度資安績效衡量表」公告資訊安全政策及目標。

3. 目標：

- 3.1. 依據資訊安全管理標準 ISO-27001/CNS-27001 驗證之精神及要求，建置與累積導入 ISMS 經驗與能力。
- 3.2. 防範本校業務運作遭受資訊安全事件之影響，並保障本校資訊系統中各項資產均能達成機密性、完整性與可用性的要求。
- 3.3. 確認網路管理相關應用系統正確執行，業務處理符合資訊網路組及校務資訊組需求，程式原始碼保管及進出管控完善。
- 3.4. 確保資訊機房安全管理周全，各項軟硬體設施保管及進出管控完善。

4. 範圍：

本校建置資通安全管理系統之實施範圍，涵蓋本校所有管理之系統和設備的日常操作、機房實體環境管理、應用軟體開發、資料儲存管理、人員安全管理等各種層面。範圍內之資訊資產泛指相關之資料紀錄和文件、電腦主機與相關資訊設備、實體運作環境、所屬之人員及各種應用軟體系統等，其適用範圍如下：

4.1. 實體資產：

4.1.1. 實體環境：本校。

4.1.2. 硬體設備：

4.1.2.1. 資通設備：電腦、防火牆主機、Domain Server、Web Server、FTP Server、Radius Server、入侵偵防系統主機、頻寬管理器等。

4.1.2.2. 網路設備：實體網路、ROUTER、SWITCH 等。

4.1.2.3. 儲存媒體：硬碟、光碟片、磁帶。

4.1.3. 支援設備：不斷電系統、電源供應器、空調設備、溫溼度計與門禁管

	義守大學 ISO-27001 資訊安全管理系統					
	文件名稱	資訊安全政策	文件編號	P9-01	制/修訂日	2024.06.25
			版次	第 2.2 版	頁次	2/7

制設施等

4.2. 資訊/資料：

4.2.1. 程式原始碼資料。

4.2.2. 每日操作重要紀錄、程式管理相關管制單、各項作業管理要點所包含之表單、制度文件及各式紀錄等。

4.3. 軟體：

4.3.1. 校務系統及其他應用資訊系統。

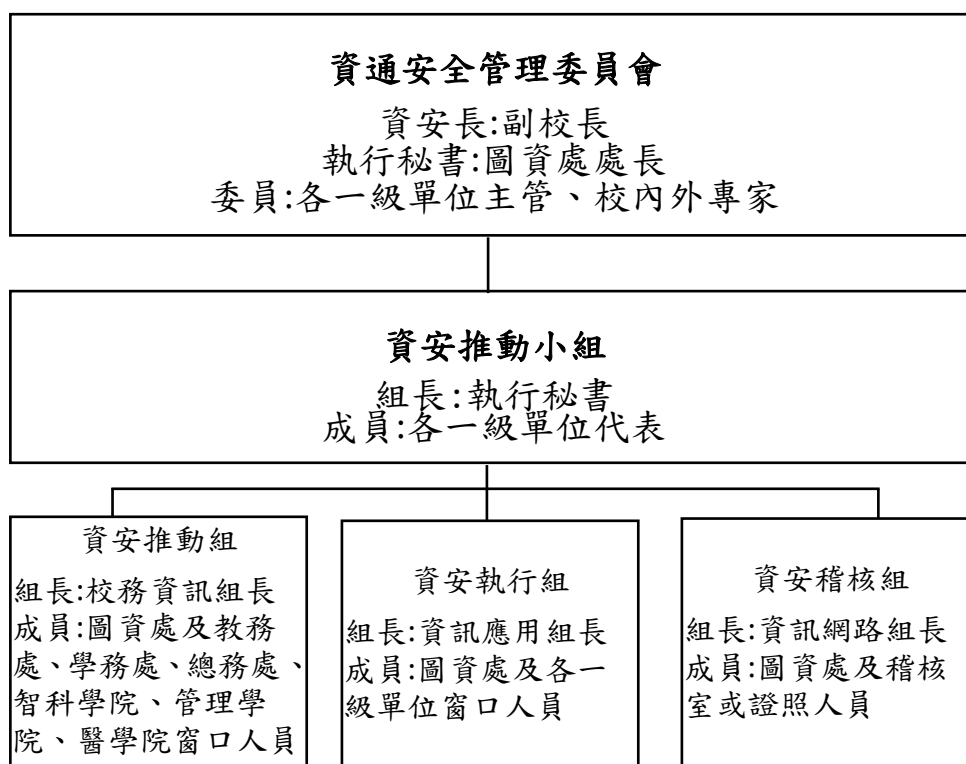
4.3.2. 網路管理應用系統(Domain、Web、FTP、Exchange、Radius、防毒軟體、入侵偵防軟體)。

4.3.3. 電腦作業系統。

4.4. 人員：各級主管、系統管理人員、系統執行人員、機房操作人員、行政作業人員、委外駐點人員。

5. 權責：

5.1. 組織架構。



		義守大學 ISO-27001 資訊安全管理系統			
文件 名稱	資訊安全政策	文件編號	P9-01	制/修訂日	2024.06.25
		版次	第 2.2 版	頁次	3/7

5.2. 工作職掌：

為推動本校之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各業務部門主管，或指派適當人員代表成立資通安全管理委員會，其任務包括：

1. 研議本校資通安全政策、目標。
2. 擬定本校年度資通安全維護計畫。
3. 規劃及推動「資通安全管理法」規定應辦或委辦事項。
4. 督導本校資通系統業務持續運作演練。
5. 規劃本校資通安全教育訓練。
6. 督導本校其他資通安全管理相關事項。

本校為強化資訊安全管理將成立推動組織，推動組織及計畫架構略述如下：

1. 資通安全管理委員會由副校長擔任資通安全長。
2. 由圖資處處長擔任執行秘書並兼資安推動小組組長。
3. 資安推動小組，下設「資安推動」、「資安執行」、「資安稽核」三組，業務推動由圖書與資訊處擔任，各一級行政單位與學院應指派一人為小組成員，擔任各單位推動之窗口，負責協助資通安全之推動、執行及稽核等相關事項。

6. 作業內容

6.1. 執行要素：

- 6.1.1. 高層支持：推動 ISMS 不僅為處理專業技術問題，更是管理制度的建立，高層管理人員將全力支持與參與。
- 6.1.2. 政策先行：推動需考量時間，確定認證與實施範圍，列出優先順序，逐步推展。
- 6.1.3. 全體共識：應使全體人員充分了解資訊安全管理制度的重要性，建立使命感，並能共同推動。
- 6.1.4. 專家輔導：建立與資訊安全專業組織與人士聯繫管道，以取得資安專家意見與已獲得認證單位意見，並善用專家經驗與能力協助本校建置資訊安全管理制度。
- 6.1.5. 教育訓練：提供適度資安教育訓練，培養同仁資訊安全管理技能。

		義守大學 ISO-27001 資訊安全管理系統			
文件 名稱	資訊安全政策	文件編號	P9-01	制/修訂日	2024.06.25
		版次	第 2.2 版	頁次	4/7

6.1.6. 定期稽核：透過內部與外部稽核程序，事前找出資安問題，提出改善建議與措施，從而降低資安風險。

6.1.7. 適時改善：發現資安議題應即時研商對策，謀求改善措施與預防事件再發生，以健全資訊安全管理制度。

6.2. 實施原則：資訊安全管理系統之實施原則，必須依據 Plan-Do-Check-Action 標準流程進行操作。：

(一)計畫

- 1.標準與法規：依據資通安全管理標準：ISO-27001/CNS-27001，做為推動與建置制度的規範。
- 2.資安教育與認知：透過資安教育訓練，使相關同仁充分了解資通安全管理制度的重要性，積極協助制度的實施。
- 3.資通安全政策訂定及評估：資通安全政策必須由高階主管審查及核准，並要求本校同仁切實遵守，以期資通安全管理成果和組織目標一致。
- 4.資通安全組織及權責：組成資通安全管理組織，應涵蓋本校內部相關組織共同運作。
- 5.風險評鑑：應用風險評鑑技術來鑑別資訊資產價值，釐清面對的威脅與漏洞、法令規章的要求，據以採取相對應之風險處理和控制措施，確保應受保護資訊的機密性、完整性及可用性。

(二)執行：

1. 風險管理：資通安全管理制度推動委員會對於風險評鑑之結果，應訂定風險可接受程度，並要求相關人員擬定風險處理計畫，限期處理。
2. 資訊資產安全管理：資訊資產應依據安全等級分類，並指定專責管理人員。
3. 人員安全管理及訓練：資訊使用人員之任用、在職及解職過程應有適當之管理機制。
4. 設備之安全管理：資訊處理設備應妥善保管，避免作業環境導致之安全風險。

 義守大學 ISO-27001 資訊安全管理系統					
文件 名稱	資訊安全政策	文件編號	P9-01	制/修訂日	2024.06.25
		版次	第 2.2 版	頁次	5/7

5. 網路通訊與操作管理：網路通訊應有標準作業程序，明定使用者及委外服務人員之責任。管理程序書應訂定系統規劃及驗收、電腦病毒及惡意軟體防範、備份管理、電腦媒體管制、資訊交換之安全管理、系統安全監控等作業規範。
6. 系統存取控制：依據本校對校務系統存取之需求，訂定使用者存取管理機制，賦予適當責任和權限，建立網路、作業系統、應用系統之存取控制措施，以及行動式電腦與電信通訊等管理機制。
7. 應用系統委外開發及操作維護：建置或採購應用系統應事先評估安全需求，系統上線後，管理人員必須遵照標準作業程序操作，並注意資料保密措施、主機日常運作及維護作業之安全性。
8. 資通安全事件管理：凡遇資通安全事件或發現系統弱點，應立即循規定管道通報主管，以即時管理和矯正資通安全事件。
9. 營運持續性管理：應訂定營運持續性管理計畫，定期演練和更新，維持緊急應變之能力。

(三)檢查：

1. 符合性：資通安全制度必須符合法規要求，管理程序和規範應依據本政策及技術符合性進行審查，並定期實施稽核，確保施行結果切合制度之要求。
2. 定期稽核：應定期進行稽核作業，稽核成果應擬具報告，由推動委員會決議後執行改善行動。
3. 懲處與責任：凡本管理制度所規範之範圍內，各相關人員未能依循制度執行業務，因而影響本校資通安全者，將依照本校相關人事規定追究責任及懲處。
4. 獎勵措施：凡本校同仁對於資通安全管理系統之實施據有良好績效者，或能提出創新積極之改善建議者，得呈報上級給予獎勵。

(四)行動：

1. 持續改善：資通安全管理為永久性之政策，圖書與資訊處全體

	義守大學 ISO-27001 資訊安全管理系統					
	文件 名稱	資訊安全政策	文件編號	P9-01	制/修訂日	2024.06.25
			版次	第 2.2 版	頁次	6/7

同仁應持續執行既定的管理程序。

2. 矯正措施：應訂定矯正及改善措施之作業程序，依據稽核審查的結果，採取矯正及預防措施，以持續改善資通安全管理作業。
3. 工作會議：資通安全代表應不定期召集各工作小組成員，舉行資通安全管理制度之工作會議，經常性檢視及討論資通安全制度之執行狀況，並適時引進管理技術，以保持資通安全制度與時代同步。

7. 審查與評估：

- 7.1. 本安全政策應依據「文件管制程序」進行修訂和發布。
- 7.2. 當適用範圍內之資產有所改變並影響原有風險評鑑基礎時，應該要對內容進行審查。
- 7.3. 本安全政策亦應針對下列情形，定期審查內容：
 - 7.3.1. 根據已紀錄的安全事件性質、次數及衝擊之顯示，檢視政策的有效性。
 - 7.3.2. 控制措施在營運效率上的成本及衝擊。
 - 7.3.3. 對技術變化的影響。