文件編號： AS-01-001

文件名稱：資訊安全政策

出 版 者：大葉大學-電算中心

機密等級：一般

使用本政策前，請先至ISMS管理系統確認版次。

本文件歷次變更記錄：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版次 | 修訂日 | 修訂者 | 說 明 | 核准者 |
| V1.0 | 97/9/22 | 江國位 | 初版發行 | 吳清沂副校長 |
| V1.1 | 97/11/07 | 江國位 | 修正資通安全事件每年發生率低於8次新增「教育體系管理規範」 | 吳清沂副校長 |
| V2.0 | 98.12.09 | 江國位 | 一、參照行政院資通安全會報及教育部公文之條文修正，資安等級分級應依照可用性、機密性、完整性做分級。二、修正資安事件定量化目標值。三、將教育部之教育體系資訊安全管理系統所定義之範圍(學術網路系統以及行政資訊系統兩大業務範疇)納入本校資訊安全政策之範圍(定義)。 | 吳清沂副校長 |
| V2.1 | 103.10.1 | 江國位 | CNS27001資訊安全管理系統於103年4月24日公布新版，驗證單位於103年10月開始受理新版稽核驗證，依據最新版本標準，修正條文內容。 | 陳明印副校長 |
| V2.2 | 103.12.15 | 江國位 | 定量化政策參照「國家資通安全通報應變作業綱要」及本校「資通安全事件緊急通報及應變辦法」資安事件影響等級修正。 | 陳明印副校長 |
| V2.3 | 105.02.15 | 吳凰庭 | 依外稽建議刪除5.1、5.2以避免過度揭露主機及系統資訊，遭駭客攻擊。 | 陳明印副校長 |
| V2.4 | 106.01.01 | 吳英傑 | 依105年11月1日資訊安全政策討論會議之決議，並提交管理審查會議中討論後，進行修正資訊安全政策之內容 | 葉釋仁副校長 |
| V2.5 | 112.10.26 | 江怡慧 | 依教育部要求大專院校須全機關導入「ISMS」，進行修正資訊安全政策之內容 | 葉釋仁副校長 |

本政策由資訊安全小組負責維護作業。

目 錄

[1 目的 1](#_Toc149220961)

[2 依據 1](#_Toc149220962)

[3 資訊安全目標 2](#_Toc149220963)

[4 資訊安全政策期許 3](#_Toc149220964)

[5 適用範圍 4](#_Toc149220965)

[6 權責 4](#_Toc149220966)

[7 資訊安全政策之遵循 5](#_Toc149220967)

目的

為維護大葉大學（以下簡稱本校）電腦機房正常營運及為保護本校核心業務相關資訊資產之安全與管理，防範資訊處理作業過程發生影響資訊及系統機密性、完整性及可用性之安全事件，確保本校資訊處理作業能安全有效地運作，特制訂資訊安全政策（以下簡稱本政策）。

依據

本政策係依據本國法律、法規、教育機構資訊安全相關文件及本校相關法規與辦法，考量相關業務需求訂定。

資訊安全目標

**資訊服務持續不中斷**

 **資訊保護嚴密不外洩**

為達成上述目標，本校資訊安全政策要求如下：

1. 利害關係團體與內外部議題之努力：
2. 全景與範圍對應其重要業務流程之要求與維運持續。
3. 達成與資安政策一致之預期。
4. 透過可量測的規範進行風險管理過程。
5. 本校之業務活動執行須符合相關法令或法規之要求。
6. 定量化政策包括：
	* + 1. 確保機房內核心系統服務達到全年99%以上之可用性。
			2. 資通安全事件等級4每年發生次數不得超過3次，等級3每年發生次數不得超過於4次。
			3. 確保相關之資訊安全措施或規範符合現行資訊安全管理標準、營運及相關法律與法規之要求（每年至少查核一次）。
			4. 維護、測試業務永續經營計畫之可行性（每年至少測試一次）。
			5. 建立資訊資產風險評估作業，至少每年進行一次風險評估。
			6. 防火牆政策檢核以確認其完整性，每半年至少做1次。
			7. 為確保校務行政資料庫之機密性及完整性，每年發生資料遭未經授權竄改之事件應為0件。

資訊安全政策期許

為達本校對資訊安全維護的期許與要求，本校將以本政策為基礎，依據組織發展需要，並考量資訊資產風險，建立一個完整、可行、有效之資訊安全管理系統，以為本校資訊安全提供最佳之保障，組織期許目標達成宜透由實際執行事項、相關負責人員、預計完成時間與執行成果評估之行動。

適用範圍

 適用範圍涵蓋本校全機關。

權責

* 1. 本校所有同仁應積極參與資訊安全管理系統（ISMS）活動，提供對資訊安全管理系統（ISMS）之支持。
	2. 成立資訊安全組織統籌資訊安全事項推動。
	3. 本政策應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性及適用性。
	4. 本校應透過適當程序落實本政策之要求。
	5. 本校高階主管應積極參與ISMS活動，提供對ISMS之支持及承諾，並適時覆核本政策。
	6. 資訊安全組織人員都有責任透過適當通報機制，通報所發現之資訊安全意外事故或可疑之資訊安全弱點。
	7. 委外服務廠商須依照合約規範或相關安全管理程序以維護資訊安全政策。
	8. 資訊安全組織組織圖：



資訊安全政策之遵循

本校所有同仁、服務廠商未遵循本政策或相關資訊安全規定，或行使其他任何危及本校資訊安全之行為，都將訴諸適當之懲罰程序或法律行動；對於資訊安全法令或技術提供改進意見，經執行確具成效者，應給予適當獎勵。