

機密等級: ■公開 □內部使用 □敏感 □密

新夥伴科技股份有限公司

資訊安全政策

文件編號	ISMS-1-00001
發行日期	2026-04-30
修訂日期	
版本	V1.0

管理代表:	Kevin
-------	-------

版本記錄

版本	日期	修訂說明	備註
1.0	2026-04-30	初版	

目 錄

1.	目的	4
2.	目標	4
3.	聲明	4
4.	適用範圍	4
5.	涵蓋內容	4
6.	組織與權責	5
7.	實施原則	5
8.	審查與評估	5

1. 目的

新夥伴科技股份有限公司(以下簡稱本公司)鑑於資訊安全乃維繫各項服務安全運作之基礎,更對品牌信譽有重要的意義,特訂定本政策,宣示本公司提供安全無虞之服務的決心與承諾,並作為本公司資訊安全工作之指導方針,以保護本公司重要資產免受內部或外部,蓄意或意外之威脅。

2. 目標

本公司資訊安全目標為:建置符合國際標準所要求之資訊安全管理系統(Information Security Management System, 以下簡稱 ISMS),確保各項服務符合機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)與適法性(Compliance)之要求。並依各階層與職能定義及量測資訊安全績效之量化指標,以確認資訊安全管理系統實施狀況及是否達成資訊安全目標。

3. 聲明

以簡單、容易記憶且符合資訊安全管理目標為原則,特訂定本公司資訊安全政策聲明為:「落實資通安全,嚴密守護數據,確保服務持續營運」。

4. 適用範圍

4.1. 本資訊安全管理系統考量內部及外部議題、關注方之需要與期望,以及本公司活動與其他組織活動間之介面及相依性,適用範圍為本公司:「N-Cloud、N-Reporter、N-Probe、N-AI、N-Ticket 之軟體開發流程及資訊基礎設施維護」。

5. 涵蓋內容

資訊安全管理系統包括內容如下,有關單位及人員就下列事項,應訂定對應之管理規範或實施計畫,並據以實施及定期評估實施成效:

- 資訊安全組織與管理審查
- 風險管理
- 文件與記錄管理
- 資訊安全內部稽核
- 人力資源安全管理
- 資產管理
- 存取控制管理
- 實體與環境安全管理
- 運作安全與密碼學技術管理
- 通訊安全管理
- 系統獲取、發展與維護管理
- 供應商關係管理
- 資訊安全事故管理
- 營運持續管理
- 遵循性管理
- 雲端服務管理

6. 組織與權責

為確保資訊安全管理系統能有效運作,應明定資訊安全組織及權責,以推動及維持各類管理、執行與查核等工作之進行。

7. 實施原則

資訊安全管理系統之實施應依據規劃(Plan)、執行(Do)、查核(Check)及調整(Act)流程模

式，以週而復始、循序漸進的精神，確保資訊業務運作之有效性及持續性。

8. 審查與評估

- 8.1. 本文件應至少每年評估審查一次，以反映相關法令法規、技術、業務及相關部門等最新發展現況，確保資訊安全實務作業之有效性。
- 8.2. 本文件應依據審查結果進行修訂，並經本公司負責人簽核發佈後始生效。
- 8.3. 本文件訂定或修訂後應以書面、電子郵件、文件管理系統或其他方式告知利害關係人，如：所屬員工、契約客戶、供應商、合作夥伴等。