|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 發行日期 | 修訂摘要 | 頁數 |
| 01 | 2023/12/29 | 初版 | 4 |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 文管人員 | 執行秘書(管理代表) | 資通安全長 |
| 文管人員 | 審核人員 | 決行人員 |

🖳 **管制文件，嚴禁私自複（影）印及繕修。**

|  |
| --- |
| 1. 目的：

為確保本公司所屬之資訊資產之機密性、完整性及可用性，並符合相關法令法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，以保障本公司之權益。1. 範圍：

資通安全管理涵蓋14項安全領域；避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來各種可能之風險及危害。管理事項如下：* 1. 資通安全政策制定及評估
	2. 組織的資通安全職責與分工
	3. 人力資源安全與教育訓練
	4. 資訊資產管理
	5. 存取控制與密碼管理
	6. 密碼管理
	7. 實體與環境安全
	8. 作業安全管理
	9. 網路安全管理
	10. 資訊系統取得、開發及維護
	11. 供應商安全管理
	12. 資通安全事故管理
	13. 營運持續管理
	14. 遵循性（適法性）
1. 依據：
	1. ISO/IEC 27001:2022 (Information technology-Security techniques-Information security management systems-Requirements)。
	2. ISO/IEC 27002:2022 (Information technology-Security techniques-Code of practice for information security management)。
	3. 行政院所屬各機關資訊業務委外服務作業參考原則。
	4. 資通安全管理法。
2. 資通安全政策：

為了促使本公司各項資通安全管理制度能貫徹執行，特予聲明「**資訊保護、全體動員、資通安全、人人有責**」，以有效安全運作、監督管理、持續進行，維護本公司重要資訊系統的機密性、完整性與可用性，並特頒佈此一資通安全政策，讓員工於日常工作時有一明確指導原則，保障本公司之權益，並期許全體同仁均能了解、實施與維持，達到本公司營運的目標，資通安全政策如下：* 1. 強化資安訓練，提升資安認知

督導員工落實資通安全工作，建立「資通安全，人人有責」的觀念，每年持續進行適當的資通安全訓練，以提高資通安全意識。員工如有違反資通安全相關規定，究其權責依人員獎懲相關規定辦理。* 1. 落實資通安全，確保持續營運

由本公司全體員工貫徹執行資通安全管理制度，以保護資訊資產免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核ISMS制度的工作，確保營運持續，達到永續經營的目的。1. 資通安全目標：

本公司執行資通安全管理制度需達成之資通安全目標，詳如「20ISMS2-0003資通安全目標管理程序書」之相關規定。1. 資通安全政策內容：
	1. 本公司各項資通安全管理規定必須遵守政府相關法規（如：刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法、資通安全管理法等）之規定。
	2. 成立資通安全管理組織負責資通安全制度之建立及推動事宜。
	3. 定期實施資通安全教育訓練，宣導資通安全政策及相關實施規定。
	4. 建立主機及網路使用之管理機制，以統籌分配、運用資源。
	5. 新設備建置前，須將風險、安全因素納入考量，防範危害系統安全之情況發生。
	6. 建立重要資訊設備及環境安全防護措施。
	7. 明確規範網路系統之使用權限，防止未經授權之存取動作。
	8. 訂定資通安全管理系統內部稽核計畫，定期檢視本公司推行資通安全管理系統範圍內所有人員及設備使用情形，依稽核報告擬訂及執行矯正預防措施。
	9. 訂定營運持續管理規定並實際演練，確保本公司業務持續運作。
	10. 本公司所有人員負有維持資通安全之責任，且應遵守相關之資通安全管理規範。
	11. 資通安全管理系統文件化資訊應有明確之管理規範。
2. 責任：
	1. 本公司的管理階層建立及審查此政策。
	2. 資通安全管理者透過適當的標準和程序以實施此政策。
	3. 所有人員與外部合約供應商，均須遵守本公司資通安全管理制度(ISMS)所要求之各項程序以維護本政策各項規範。
	4. 所有人員有責任報告安全事件，和任何已鑑別出的弱點。
	5. 所有人員與外部合約供應商，若蓄意違反本公司資通安全規範及法令法規之行為，都將受到相關懲處或負法律之刑責。
3. 審查：
	1. 本政策應至少每年評估一次，以反應政府法令、技術及業務等最新發展現況，以確保它對於維持營運和提供適當服務的能力。
	2. 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。在必要時應告知相關單位及合作廠商，以利共同遵守。
4. 實施：

本政策經資通安全長(或資通安全管理代表)核准後，於公告日施行，並以書面、電子或其他適當之方式通知本公司員工及與本公司連線作業之有關廠商，修正時亦同。 |