|  |
| --- |
| 三芳化學工業股份有限公司 |
| 資通安全管理政策 |
|  |

|  |
| --- |
| 經營管理處 資訊室2022/4/19版本1.0 |

目錄

[壹、 目的 2](#_Toc101260716)

[貳、 資通安全政策目標 3](#_Toc101260717)

[參、 資通安全政策內容 4](#_Toc101260718)

[肆、 風險管理架構 5](#_Toc101260719)

[伍、 具體方案 6](#_Toc101260720)

[陸、 投入資通安全管理之資源 7](#_Toc101260721)

[柒、 重大資安事件 8](#_Toc101260722)

## 目的

 為維護本公司永續運作與經營，遵循相關法令法規，避免遭受內外部竄改、加密、揭露、破壞或遺失等威脅，確保資訊資產之機密性、完整性、可用性，依照法規訂定公司資通安全政策、具體管理方案及投入資通安全管理之資源等，作為資通安全管理之準則與遵循依據。

## 資通安全政策目標

本公司資訊安全政策訂有下列目標：

1. 確保資訊流程持續運作，資訊服務穩定運行。
2. 落實資訊安全法令，建立完善資訊安全措施，維護資訊環境安全。
3. 維護組織商業資產之機密性、完整性與可用性。

## 資通安全政策內容

本公司資訊安全政策內容如下：

1. 制定資訊設備使用與安全管理辦法，供使用者遵循與規範。
2. 健全資安設備，定期檢視與更新。
3. 建立完善的異地備援架構，定期備份與還原演練。
4. 加強人員資訊安全知識，定期提供相關訊息。
5. 定期社交工程演練，強化內部資安意識。
6. 落實設備定期系統更新，確保內部安全等級。
7. 建立主動與被動之防護機制。
8. 落實資訊分級制度，機密資料加密保護，確保公司與客戶資訊權益。

## 風險管理架構

本公司資訊安全之權責單位為經營管理處資訊室，負責制定資訊安全政策與落實各項資訊安全管理要求。當年度結束前針對資訊安全進行風險性評估，採循環式管理，依照風險危害等級提出各項具體改善計畫，落實執行、查核工作進度、後續追蹤與改善，以達成資訊安全之目標。

另鑒於外在威脅技術不斷推陳出新，委請外部專業資安團隊協同強化防禦，客觀評估內部風險，針對弱點進行改善措施與定期追蹤進度，降低資安風險。

## 具體方案

具體管理方案分三個方向進行：

1. 外部資安團隊：

外在威脅變化迅速，引進專業資安團隊協同防護。外部資安團隊依照主動偵測防護系統隨時監控主機資安狀況，針對內外部威脅提出改善建議，依照風險性等級不同採取個別措施，風險性高則立即提出改善建議，內外協同執行，過程隨時回報與追蹤。

1. 內部風險管理：

資訊室針對各項風險採循環式管理，落實內部查核，評估人為操作、天然災害及惡意網路攻擊對資訊資產與服務之風險，再針對資訊系統架構其風險等級建立服務高可用性架構、資訊備援服務及資料備份機制，並訂定災難復原計畫與定期演練，以確保公司業務持續運作。內部稽核單位亦定期辦理資通安全檢查與釣魚信件演練，並將演練結果呈報上級，亦定期向董事會呈報相關內控稽核報告。外部會計師也會查核資訊系統風險控管，包含系統權責劃分、資料安全管理、實體與環境安全管理、流程稽核等資訊風險予以評估，並向呈報缺失與改善方案。

1. 員工資安訓練：

針對外來設備管控與員工資訊安全知識不足之處進行宣導與要求，另每年定期進行社交工程演練，提升內部資安意識。針對無法落實部分則列入風險，提出有效改善措施。

## 投入資通安全管理之資源

具體投入資源如下：

* 1. 防火牆設備。
	2. 主動偵測設備。
	3. 端點防護軟體。
	4. 郵件過濾機制。
	5. 專用備份主機與異地備援。
	6. 一年兩次社交工程演練。
	7. 一年一次重要主機災害復原演練。
	8. 外部資訊安全維護服務。

## 重大資安事件

目前公司雖可自行辨認及揭露其資通安全風險暴露情形，惟為落實公司對資通安全之風險揭露，爰明定公司應揭露資通安全風險對公司財務業務之影響及因應措施，及因重大資通安全事件所遭受之損失、可能影響及因應措施。

截至年報刊印日止並無資安問題發生。