興采實業資通安全政策

1. 引言

本公司深知資通安全對業務運營的重要性，為保障資訊系統和數據的安全，特制定本資通安全政策，以明確相關的管理原則和措施。

2. 政策目的

2.1 確保資訊系統和數據的保密性、完整性和可用性，防止未經授權的訪問、使用或披露。

2.2 預防、監測和應對資訊安全事件，以減輕可能的損失。

2.3 遵守相關法規和法律，保護公司和客戶的權益。

3. 執行範圍

本政策適用於公司內所有的資訊系統、數據和相關人員。

4. 主要原則

4.1 資訊保密性：

所有員工必須嚴守資訊保密原則，不得將公司機密信息外洩或提供給未經授權的人員。

4.2 資料完整性：

確保數據的完整性，防止未經授權的修改、刪除或損壞。所有修改需經過授權和記錄。

4.3 服務可用性：

確保資訊系統的穩定運行，及時應對可能影響系統正常運營的事件，並建立相應的緊急應變機制。

4.4 風險評估與控制：

定期進行風險評估，制定相應的風險控制措施，保障資訊安全。並建立風險評估報告，提供給相關主管和委員會。

4.5 員工培訓與教育：

提供定期的資訊安全培訓和教育，包括但不限於新員工培訓、風險意識提升、安全技能培養等，提高員工對資訊安全的認識和應對能力。

5. 資通安全控制措施

5.1 身份認證和訪問控制：

確保只有經授權的人員可以訪問特定的資訊系統和數據，並建立相應的身份認證機制，包括強化密碼複雜度要求和定期更換策略。

5.2 加密技術應用：

對敏感信息進行加密，保障信息在傳輸和存儲過程中的安全。

5.3 防火牆和入侵檢測系統：

部署防火牆和入侵檢測系統，防止未經授權的訪問和攻擊。

5.4 安全更新和漏洞修補：

定期更新和修補資訊系統中的漏洞，以保障系統的安全性。

5.5 資訊安全備份和恢復：

定期備份資訊資產，建立災害恢復計劃和應急應變預案，確保資訊的可用性和完整性。

5.6 安全事件監控和應變：

建立安全事件監控系統，即時檢測和應對安全事件，包括定期的模擬演習以提高應變能力。

6. 違規處理

如發現有員工違反本政策，將根據公司相應的違規處理程序進行處理，並進行相應的紀錄和監控。

7. 政策的修訂與實施

7.1 本政策的修訂及實施，須經董事會批准，並通知相關部門及人員。

7.2 公司將持續評估資通安全政策的有效性，並根據需要進行相應的調整。