

國統國際股份有限公司

資通安全政策

一、資通安全目的：

1. 確保公司主機、網路設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資通安全管理規範。
2. 確保公司業務資訊之機密性、完整性與可用性。
機密性：確保被授權之人員才可使用資訊。
完整性：確保使用之資訊正確無誤、未遭竄改。
可用性：確保被授權之人員能取得所需資訊。

二、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：資通安全管理法、刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法等）之規定。
2. 成立資通安全管理專職單位，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. 新系統及設備建置上線前，須將風險、安全因素納入考量，防範危害資通安全之情況發生。
6. 建立資訊機房實體及環境安全防護措施，並定期施以相關維護及保養。
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. 訂定資通安全管理制度內部稽核計畫，定期檢視資通安全管理制度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. 訂定營運持續管理備援/備份還原之演練，確保公司業務持續運作。
10. 本公司所有人員負有維持資通安全之責任，且應遵守公司相關之資通安全管理規範。
11. 委外廠商在執行本公司委外業務時若有複委託之需求，應評估複委託業務相關之資安風險。並要求委外廠商依資通安全相關規定對複委託廠商進行適當之監督與管理。
12. 對內部及外部專案管理的過程中，應明訂及陳述與專案相關之各項資通安全要求，確保內部及外部專案資訊之機密性、完整性及可用性，降低機敏資訊(含個人資料)外洩及違反法令之風險。
13. 資安政策之評估與審查應至少每年評估及審查一次，以反映管理政策、政府法令、新科技技術及公司業務等之最新發展現況，確保資通安全管理制度的可行性及有效性，以維持營運和提供適當服務的能力。

三、 資通安全管理機制

為確保公司治理的穩固性、降低營運風險，並提供卓越的客戶服務，資通安全管理機制，包含以下三個面向：

1. 建立一個完備的資訊安全管理體系。以保護公司的重要資訊資產，實現長期的經營目標。
2. 強化電腦機房和網路管理，
3. 定期實施員工資訊安全訓練：進行資通安全教育訓練，提昇全體同仁資安意識。

四、 鑑別可能的資安威脅：

近來新興科技與商業模式的轉變，也帶來新型態的資安威脅，主要項目包括：

1. 天然災害：包括火災、地震、水災、颱風等自然災害，可能對業務運作和設施造成損害。
2. 機房設施失效：指不斷電系統、電力或冷氣空調等設施的故障或失效，可能導致系統中斷或損害。
3. 系統異常：包括硬體設備故障，如主機故障，以及硬體障礙，可能導致系統功能受損。系統、軟體異常：指資料庫服務、ERP 系統等軟體的異常，可能導致業務中斷或資料損失。
4. 網路異常：指網路中斷，如網路無法連接或對外網路無法連接，可能對通信和連接性造成困擾。
5. 駭客入侵：指駭客攻擊，如加密勒索、DDoS 攻擊等，可能導致系統損壞或中斷。
6. 人為操作失當：包括執行人員未遵守相關作業程序，可能導致操作失誤或風險增加。
7. 廠商維修及維護人員未依規定執行評估及風險控管作業：指外部廠商或維護人員未按照規定執行維護作業，可能導致風險增加。
8. 人為蓄意破壞、無意疏失、洩漏機敏資料或違反資安規範之行為：包括故意或無意的內部人員行為，可能對資訊安全造成威脅。
9. 電腦或週邊失效：指個人電腦設備、硬體、軟體、作業系統、電力、網路失效，或週邊設備故障，可能對工作效能造成困擾。
10. 設備失竊：指公司的設備遭到竊取，可能對資訊安全和業務運作造成風險。
11. 一般電腦中毒：指電腦受到病毒或惡意軟體感染，但未造成服務異常或中斷。

五、 資通安全風險管理架構：

為因應各項潛在的資訊安全威脅，降低風險發生的機率並減輕潛在影響，遵循金管會「公開發行公司建立內部控制制度處理準則」的要求下，設立了專門的資訊安全專責單位『資安室』，包括一名資安專責主管以及至少一名資安專責人員。在制度方面，我們參考了上市櫃公司資通安全指引的相關程式，以不斷改善和強化國統的資訊安全管理體系。

透過風險評鑑和資訊安全稽核作業，我們致力於識別和評估高風險事項，並採取相應的管理措施。這些舉措旨在減少資訊風險發生的可能性，以及最小化其潛在影響。我們的目標是確保公司能夠持續營運，並保護客戶和股東的資訊和利益，同時遵守相關的監管要求。

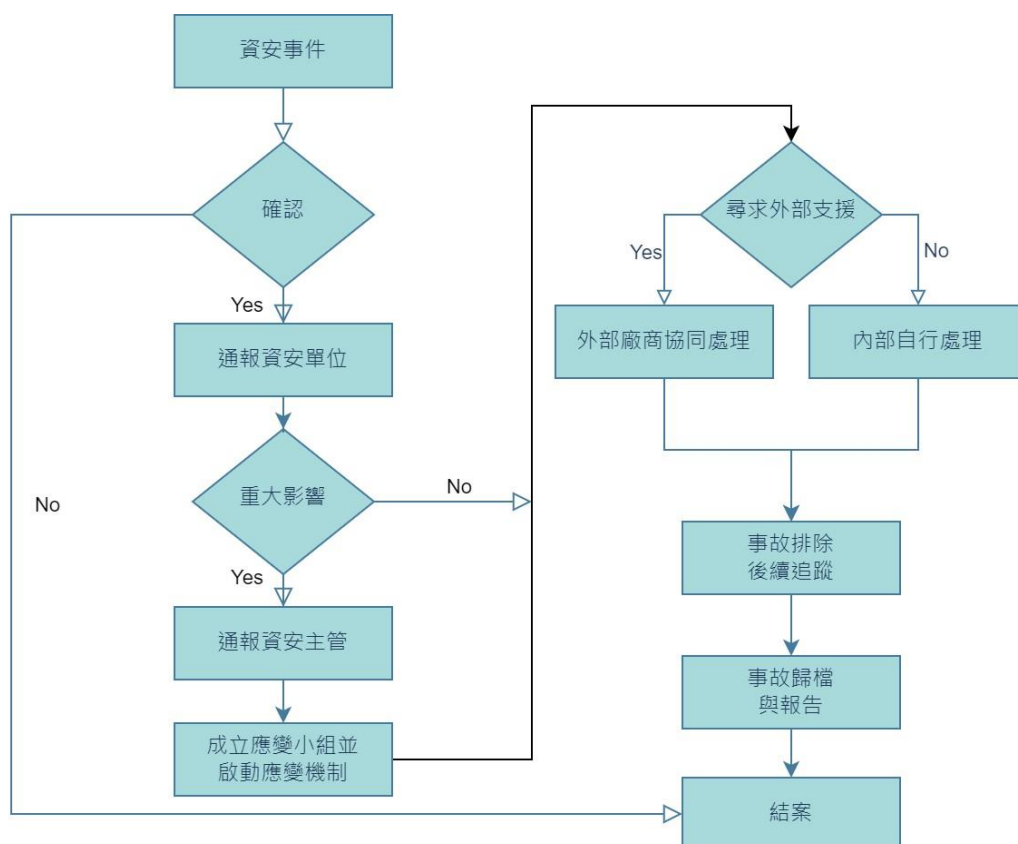
六、 資通安全防護及管理措施：

在技術和系統面，也導入各項資安的防護措施，以減少威脅並進行風險管控，本公司實施資通安全管理措施如下：

每年進行社交工程攻擊模擬演練，並提供資安教育訓練，以提高員工對郵件安全的警覺性。

1. 伺服器 and 個人電腦配備防毒軟體，並自動定期進行病毒和惡意程式掃描，以確保電腦安全。
2. 使用 M365 郵件過濾和郵件稽核系統，以減少電子郵件受到攻擊的風險。
3. 使用 NAS 建立差異化異地備份系統，確保重要資料的安全性。
4. 在 Internet 網路上設置實體式防火牆，以控制網路流量和應用程式。
5. 建立檔案監控系統，紀錄檔案異動資訊，並防止文件遭到大量複製或修改。
6. 主機集中管理，建立機房溫度監測系統，定期進行資料備份，並每年進行資料復原演練。
7. 在各種資訊系統中實施多層次的權限和密碼管理，以確保使用者的合法性。
8. 實施遠端加密連線(SLL VPN)作業，並要求使用端電腦透過 VPN 連結內部網路時，須先檢查是否為公司網域內之電腦及並且已安裝指定之防毒軟體，否則拒絕連結。
9. 定期執行稽核作業，除作為改善資安系統運作依據外，並可以精進資安管理體系運作之成效。

七、 資通安全通報程序：



八、 在資訊安全風險的管理作業上，需要不斷地遵循 PDCA (Plan-Do-Check-Act，計劃-執行-檢查-行動) 的方法，並不斷精進資訊安全措施，本政策應每年評估及審查一次。