立積電子股份有限公司

資訊安全風險管理政策與程序

一.資訊安全目的與範圍

1. 對象: 包括員工，客戶，供應商和股東以及營運相關資訊軟硬體設備。
2. 範圍：為確保本公司資訊安全，制定相關規章制度，應用技術和數據安全標準制定，並納入管理運作體系，以保障員工，供應商和客戶進行業務接洽時之隱私權保護與資訊安全維護。

二. 資訊安全風險架構

1. 由本公司總經理召集成立跨部門資訊安全管理小組，資訊部門與行政管理部門負責主導及規劃，各業務相關單位配合執行，以確認本公司資訊安全管理運作之有效性。
2. 本小組負責制定資訊安全管理政策，定期至少每年一次檢討修正。
3. 本小組定期召開會議檢討執行情形，並每年定期至少每年一次向董事會報告執行情形與檢討。

三. 資訊安全政策目標

1. 確保本公司營運業務持續運作，且本公司提供的資訊服務可穩定使用。
2. 確保本公司所保管的資訊資產之機密性、完整性與可用性，並保障人員資料之隱私。
3. 建立資訊業務永續運作計畫，執行符合相關法令或法規要求之資訊業務活動運作。

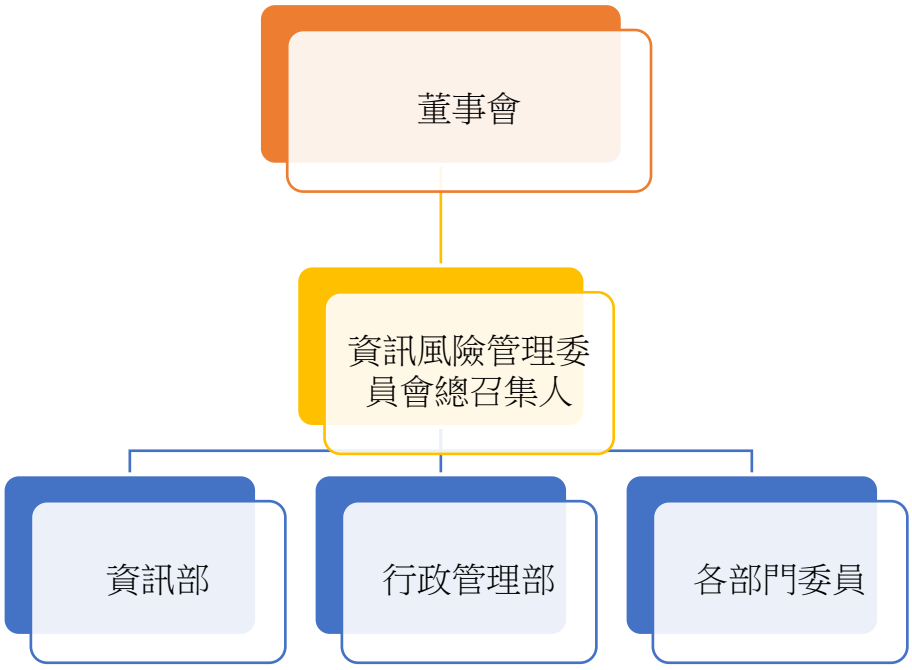
四. 資訊安全控制措施

1. 建立每年定期盤點資訊資產清單，依資安風險評鑑進行風險管理，落實各項管控措施。
2. 公司定期執行資訊安全宣導作業，每年至少一次辦理資訊安全教育訓練，新進人員皆須簽定資訊保密協定。
3. 本公司所有員工、委外廠商暨其協力廠商須簽定保密聲明書，已確保使用本公司資訊以提供資訊服務或執行相關資訊業務者，有責任及義務保護其所取得或使用本公司之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。
4. 重要資訊系統或設備應建置適當之備援或監控機制並定期每年至少一次演練，維持其可用性。
5. 個人電腦應安裝防毒軟體且定期確認病毒碼之更新，並禁止使用未經授權軟體。
6. 同仁帳號、密碼與權限應善盡保管與使用責任並定期換置。
7. 制定資訊安全事件的回應及通報標準程序，以適當對資訊安全事件做即

時處理，避免傷害擴大。

8. 全體人員應遵守法律規範與資訊安全政策要求，主管人員應督導資安遵行制度落實情況，強化同仁資安認知及法令觀念。

五. 資訊安全管理組織



六. 實施

本政策與程序經審計委員會及董事會通過後實施，修訂時亦同。於中華民國一一〇年十二月二十三日制定。