資訊安全政策

目的：

為強化鴻呈實業股份有限公司(以下簡稱「本公司」)資訊安全管理落實，確保公司業務資訊之機密性、完整性與可用性，以符合相關法令、法規之要求，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，並建立資訊安全政策規範。

1. 機密性：確保被授權之人員才可使用資訊。
2. 完整性：確保使用之資訊正確無誤、未遭竄改。
3. 可用性：確保被授權之人員能取得所需資訊。

適用範圍：

本政策適用範圍為本公司全體同仁、委外服務廠商與訪客等。

內容：

1. 本公司各項資訊安全管理規定必須遵守政府相關法規，如：上市上櫃公司資通安全管控指引、個人資料保護法等之規定。
2. 成立資通安全推動組織，組織配置適當之人力、物力與財力資源，並指派適當人員擔任資安專責主管及資安專責人員，負責資訊安全制度之建立及推動事宜。

3. 新進人員錄用應簽署相關保密條約作業規定之文件，以確保新進同仁均了解機密文件之保護之必要性並提昇資訊安全防護之認知觀念。
4. 定期對員工實施資訊安全教育訓練，除宣導資訊安全政策及相關實施規定，需確保員工有足夠之資訊安全意識。
5. 公司所有人員負有維持資訊安全之責任，並遵守公司相關之資訊安全管理規範。
6. 制定資訊安全管理制度內部稽核計畫，稽核人員須定期檢視資訊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。
7. 資訊安全政策之評估與審查應至少每年評估及審查一次，以確保政策符合政府法令、公司業務等之最新發展現況，確保資訊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。
8. 新系統及設備建置上線前，須將風險、安全因素納入考量，必須通過安全檢測，避免危害資訊安全之情況發生。
9. 所有資訊系統皆必須設定密碼才能進行操作，使用者密碼應符合安全原則，並要求定期更改通行密碼。人員暫時離開或下班時應將電腦鎖定或是登出系統後關機。
10. 資訊機房實體及環境安全防護，定期檢查維護及保養。
11. 訂定災難復原管理/備份演練，確保公司業務持續運作無虞。
12. 建立各主機及網路使用之管理機制，禁止員工自行攜帶、架設網路串接至公司內部網路設備。
13. 為確保公司資訊安全，公司透過防火牆、入侵偵測及防毒軟體等相關系統的建置，阻擋病毒及入侵攻擊公司內部網路。另建立評估各系統的漏洞並針對主機、設備進行漏洞修補，以有效防止病毒與駭客透過系統漏洞，進行攻擊。

14. 委外廠商在執行公司委託之委外業務時，應評估委託業務相關之資訊安全風險。並要求委外廠商依資訊安全相關規定履行或嚴守相關之管理規定。
15. 對專案管理應明訂專案相關之各項資訊安全要求，確保專案資訊之機密性、完整性及可用性，降低機敏資訊外洩及違反法令之風險。
16. 同仁遇有資訊安全事件，應立即通報資訊部門，避免事件擴大，並配合權責部門共同解決。