鼎基先進材料股份有限公司

資訊安全管理內部控制制度(第一版)

第一條　目標

提供本公司之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

此政策規範由最高管理階層擬定，藉有效的系統運作，包含各流程持續改善，以預防不符合事項，以達到資訊安全之目的。

維護本公司資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標：

一 保護本公司業務活動資訊，避免未經授權的存取。

二 保護本公司業務活動資訊，避免未經授權的修改，確保其正確完整。

三 宣導員工資訊安全之意識與強化其對相關責任之認知。

四 實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。

第二條　組織職掌

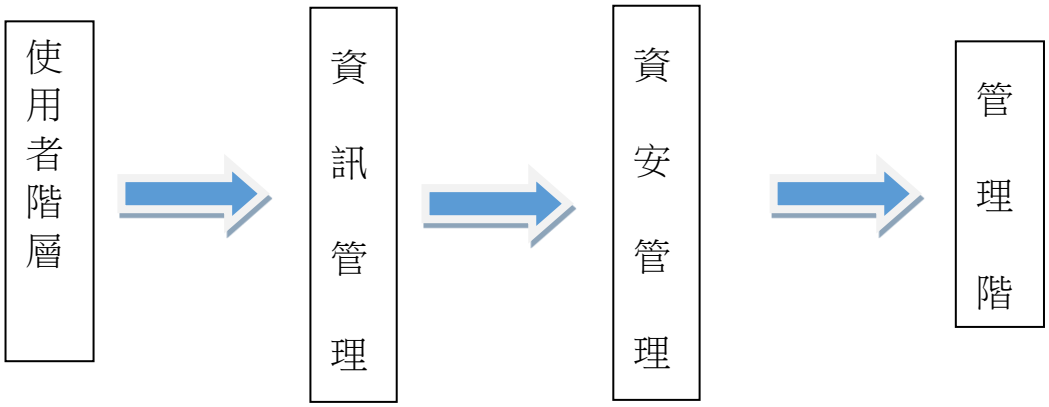
本公司之內部人員、委外服務廠商與訪客皆應遵守，且資訊系統依其職責業務區分，發生問題需層層通報。

一 使用者階層：合理操作公司系統及資訊軟體。

二 資訊管理階層：權限設計及控管、備份計畫執行、防毒、防駭策略擬定及執行、合法軟體安裝及控管、等…。

三 資安管理階層：資訊安全策略設計規劃、資安風險控管。

四 管理階層：掌控構面的衝擊程度，設定安全等級。



第三條　分層負責明細表

層級	職務	工作項目	備註
第一級	一般使用者	依公司規定合理操作資訊系統及資訊軟體、網路服務。	例：作業員、外部人員
第二級	資管人員	備份計畫、防毒、防駭策略之執行，及合法軟體安裝及控管。	MIS
第三級	資安主管	資安風險管控。	資安部門
第四級	稽核及 關鍵主管	設定資安目標等級	
第五級	總經理	掌控公司內部的衝擊程度及影響評估	
第六級	董事會	掌控公司外部的衝擊程度及影響評估	

第四條　資安等級

等級	衝擊或後果	事件	備註
1	輕微	個人電腦事件，沒有公司資料外洩、毀損	
2	低	單一員工或系統事件，資料輕微毀損但無外洩，短時間內回復功能。	經費/時間輕微增加
3	中	多員工、部分系統事件，資料毀損、外洩，長時間方能回復功能	經費/時間中度增加
4	高	多員工、全系統事件，資料毀損、外洩，無法回復功能。造成公司業務停頓中斷。	經費/時間大量增加

第五條　控制作業

各項控制作業，係為確保各項業務活動皆已有效運作，相關控制重點已併入各項業務活動之作業流程中設計，包括合法軟體管理、權限設計及控管、備份計畫、備援計畫、防毒策略、防駭策略、行動裝置管理等...

第六條　資訊安全之監督實施方式

一 由內部各單位主管例行督導各項資安業務。

二 每年單位自行檢查一次內部控制制度設計及執行之有效性。

三 單位進行內部資訊安全查核。

四 不定期稽核人員至資訊單位進行資安稽核。

第七條　使用者存取權限覆核

為有效控管資料及系統存取，視需要不定期檢討及評估使用者之存取權限。

第八條　作業系統更新

作業系統變更之技術評估

一 作業系統視需要不定期更新(例如安裝新的版本)；作業系統變更時，應評估其對應用系統是否造成負面的影響，或是產生安全問題。

二 作業系統變更之評估程序，應考量的事項如下：

1. 評估公司管理系統不受作業系統變更而影響。
2. 作業系統的變更應即時通知相關人員，以便在作業系統變更前，相關人員可以進行適當及充分的評估作業。

第九條　自行檢查

為評估機關整體內部控制制度設計及執行之有效性，應將內部控制之組成要素納入機關整體層級自行檢查表中，每年至少自行檢查一次，遇有特殊情形，得隨時辦理，其中「控制作業」一項，並應納入作業層級自行檢查表中進行檢查。

第十條　本控制制度經總經理核准後實施，修正時亦同。