	艾美特(開曼)國際有限公司	頁數：6
		檔編號：FI-31
	檔案名稱：資訊安全風險管理辦法	版本.版次：1.0
		制訂日期：2023/12/13

一、目的

為保護公司資訊資產，免於遭受自內部或外部人為、蓄意或意外之破壞，而制訂資訊安全風險管理辦法，以作為實施各項資訊安全措施之標準。

確保公司伺服器、網路設備及通訊與資訊系統的安全，規範公司伺服器、網路和資訊系統的管理，以確保系統資源高效、安全地用於工作目的，加強對公司資訊資產的安全性保護，達到永續經營目的。

1.1 確保公司業務資訊之機密性、完整性與可用性。

1.2 機密性：確保被授權之人員才可使用資料。

1.3 完整性：確保使用之資訊正確無誤、未遭篡改。

1.4 可用性：確保被授權之人員能取得所需資料。

二、適用範圍

有關資訊安全風險之事項，本公司及集團所屬子公司、分公司及各地辦事處等分支機構，委外服務廠商、訪客等，除另有規定外，悉依本辦法辦理。

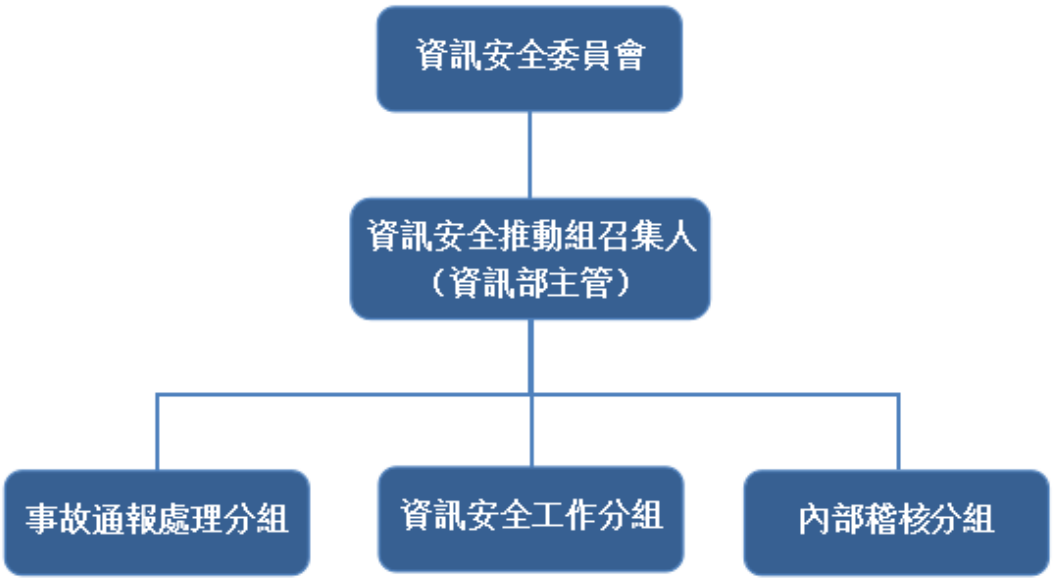
三、作業程式

3.1 資訊安全政策評估

應由具專業技術及知識之資訊單位、內部稽核單位的主管人員辦理，并定期評估。

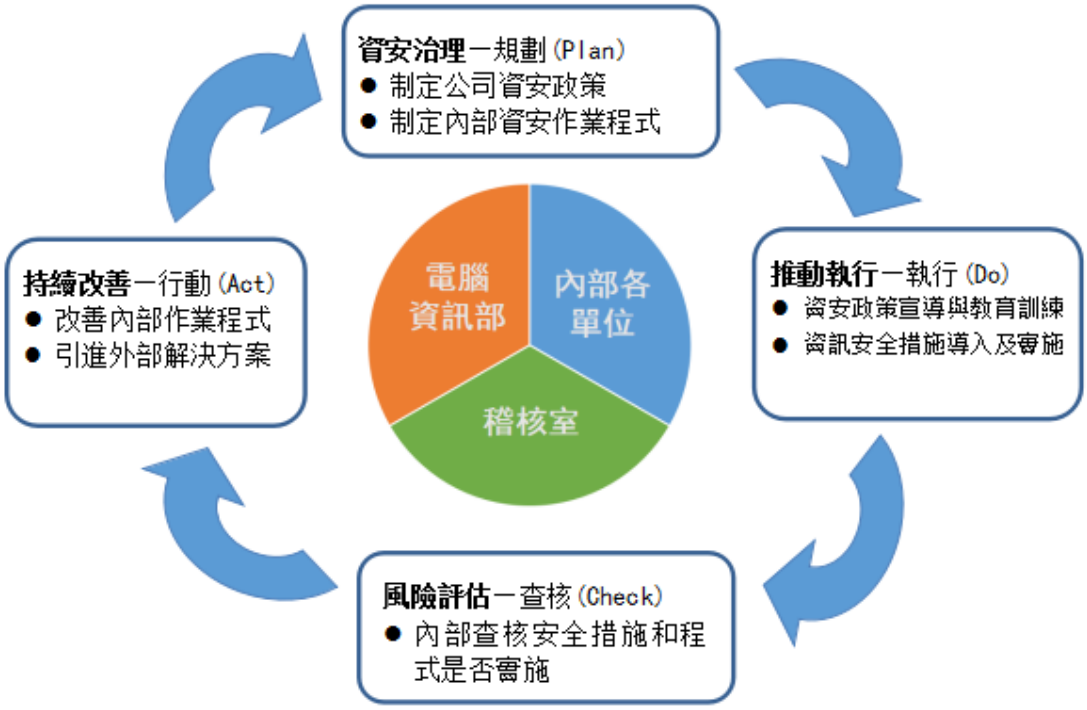
3.2 資訊安全組織與管理

為提升資訊安全風險管理與資訊安全相關政策執行與推動，由資訊委員會負責審視本公司及各子公司間資安治理政策，并監督資安管理動作情形。



資訊安全委員會	負責資訊安全政策制訂與推動，資訊安全之權責單位為電腦資訊部，由資訊部主管擔任召集人。
事故通報處理分組	負責資訊安全事件等級判斷、通報、調查、處理及改善報告
資訊安全工作分組	負責執行資訊安全作業與資訊安全風險評估
內部稽核分組	負責內部查核安全措施和程序是否實施

組織運作模式-采 PDCA（Plan-Do-Check-Act）循環式管理，確保目標之達成及持續改善。



3.3 資訊安全管理具體作業

本公司資訊安全管理具體作業，主要體現在以下幾方面：

3.3.1 電腦設備安全管理：

本公司各應用伺服器等設備均設置於專用機房，機房之門禁須採用感應刷卡進出，且保留進出記錄存查。

機房內部備有獨立空調，維持電腦設備於適當的溫度環境下運轉；並放置藥劑式滅火器，可適用於一般或電器所引起的火災。

機房主機配置不斷電與穩壓設備，避免主機意外瞬間斷電造成系統當機，或確保臨時停電時不會中斷電腦應用系統的運作。

3.3.2 網路安全管理：

與外界網路聯機的入口，配置企業級防火牆，阻擋駭客非法入侵。

配置上網行為管理與過濾設備，控管因特網的存取，可遮罩訪問有害或政策不允許的網路地址與內容，強化網路安全並防止帶寬資源被不當佔用。

3.3.3 病毒防護與管理：

伺服器與員工終端電腦設備內均安裝有端點防護軟體，病毒特徵采自動更新方式，確保能阻擋最新型的病毒，同時可偵測、防止具有潛在威脅性的系統執行檔之安裝行為。

電子郵件伺服器配置有郵件防毒、與垃圾郵件過濾機制，防堵病毒或垃圾

郵件進入用戶端的資訊設備。

3.3.4 系統訪問控制：

員工對各應用系統的使用，透過公司內部規定的系統許可權申請或軟體需求（許可權）申請程式，經權責主管核准後，由電腦資訊部建立系統帳號，並經各系統管理員依所申請的功能許可權做授權方得存取。

員工離(休)職時，工程師根據人事離職資訊進行各系統帳號的停用刪除等作業。

3.3.5 確保系統的永續運作：

系統備份: 業務數據必須完整、真實、準確地轉儲到離線的介質或備份伺服器上，並要求集中和異地保存，依照業務數據的性能設置備份數據保留年限。

災害復原演練：核心系統資料庫復原時間目標（RTO）為 24 小時，資料庫資料復原時間點目標（RPO）為 8 小時，每年實施一次對關鍵數據進行災難恢復演習，確保數據可以在規定時間內完整得到恢復。

3.3.6 資安宣導與教育訓練：

所有新進有帳號的員工，每季皆須完成員工資訊安全意識教育訓練課程和考核。宣導妥善管理個人電腦密碼，並已在系統中設置在每個週期提前要求用戶修改密碼，以維持帳號安全。

定期通過電子郵件、培訓等方式對內部員工實施資訊安全相關的教育訓練宣導。

3.4 資訊安全管理措施

本公司實施之資訊安全管理措施，其類別 / 說明 / 控制措施詳如下：

類型	說明	控制措施
許可權管理	人員帳號與許可權授權管理	● 人員帳號許可權管理與審核 ● 人員帳號許可權定期復核 ● 人員密碼定期更換
存取管控	人員存取內/外部資源、及資料傳輸控制	● 內/外部網路連線與存取管控機制 ● 電腦軟體安裝和文件存儲修改許可權管制
外部威脅	病毒入侵防護	● 定期掃描/病毒庫及時更新 ● 防火牆入侵偵測/病毒/惡意程式防護
郵件安全管理	郵件防護	● 郵件帳號和容量管控 ● 郵件病毒防護及惡意程式偵測 ● 郵件惡意連結保護，避免網路釣魚 ● 防垃圾郵件過濾
系統可用性	系統可用狀態與服務中斷預防	● 系統/網路可用狀態監控及通報機制 ● 服務中斷之應變措施

		● 本地/異地資料備份措施和機房備援 ● 每年定期災害復原演練
本公司為強化應對日新月異的資訊攻擊事件，除了透過定期檢查防火牆安全政策、防毒軟體之病毒碼定期更新、與定期備份資料於異地外，對於災害復原演練訂於每年實施一次，以確保備份機制之正常運作，並能符合系統復原目標。		

五、資訊安全事件通報程序

5.1 為加強公司資訊安全工作，及時掌握和處置資訊安全事件，協調做好應急回應處理，降低安全事件帶來的損失與影響，維護正常工作秩序，當發現資訊安全事件時，按下圖流程進行回應處置。

5.2 本公司資訊安全事件通報窗口為事故通報處理分組，相關權責人員應於知悉資訊安全事件後，依規定《信息系統與網絡事件應急預案》之資訊安全事件等級判斷：

5.2.1 事件涉及核心業務或關鍵基礎設施業務之資訊是否

5.2.2 事件導致業務之資訊或資通系統遭竄改之影響程序，屬嚴重或輕微。

5.2.3 事件所涉資訊是否屬於公司機密或敏感資訊。

5.2.4 關鍵業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內回覆正常運作。

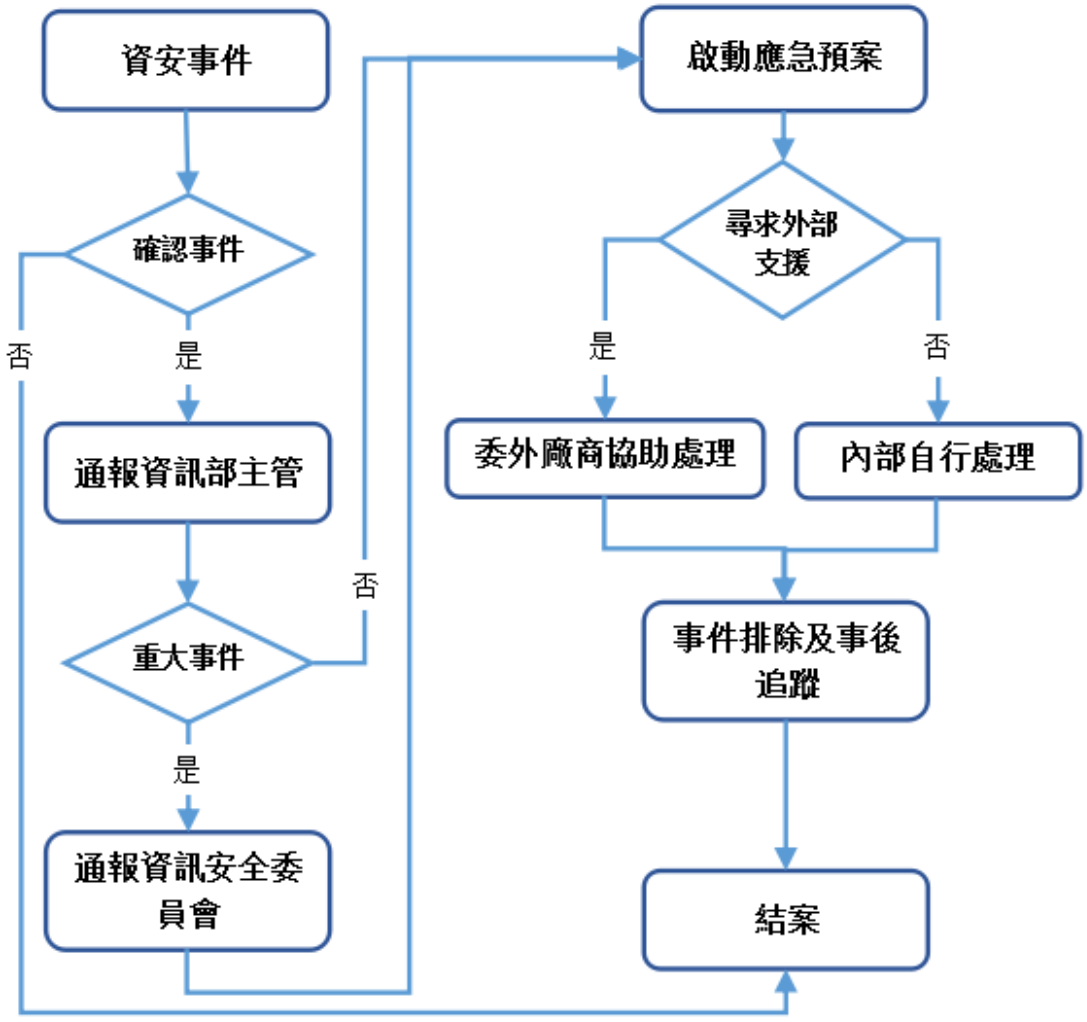
5.2.5 事件其他足以影響資訊安全事件等級之因素。

除事件之等級外，權責人員或緊急處理小組亦應對資訊安全事件之影響範圍、損害程序及本公司因應之能力進行評估。另，資訊安全事件等級如有變更，權責人員或緊急處理小組應告知通報窗口，使其續行通報作業。

5.3 本公司完成資訊安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，并應於事件發生後三個月內完成資訊安全事件調查、處理及改善報告。

六、附則:

本管理辦法經董事會通過後公佈實施，修改時亦同。


資安事件
確認事件
否
是
通報資訊部主管
重大事件
否
是
通報資訊安全委員會
啟動應急預案
尋求外部支援
是
否
委外廠商協助處理
內部自行處理
事件排除及事後追蹤
結案