P-DUKE Technology Co., Ltd.
Tel +886-4-2359-0668
Fax +886-4-2359-1338
Email sale@pduke.com
Web www.pduke.com
Add No. 36, 22nd Rd., Taichung Industrial Park,Taichung, Taiwan, R.O.C.

# 資訊安全管理

避免公司資訊資產遭受內部、外部、或有意的威脅，確保資訊的合法性、完整性、機密性與可用性，進而提供安全、穩定及高效率之整體資訊服務。並訂定資訊安全架構，降低資安風險。

1.資訊安全風險架構：

(1) 已導入防火牆設備，明確規範對外服務之服務器所需端口，其餘端口皆一律封鎖，以加強對外服務之伺服器安全。

(2) 導入 IPS(入侵防禦系統)，針對外部對內部之網路封包，皆需經過此 IPS 過濾並確認無問題後才可放行至內部網路，以確保內部主機的安全。

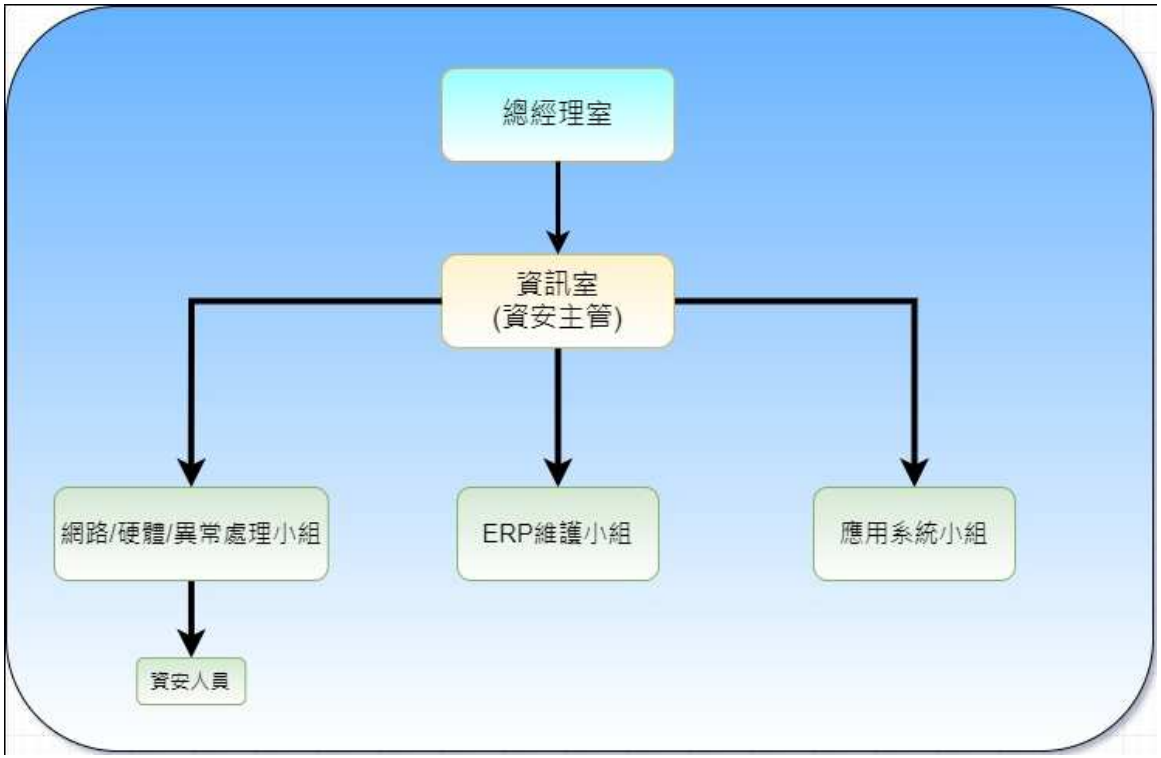
(3) 內部資安人員會不定期，進行 IPS 入侵防禦系統事件分析，會針對異常事件向資安廠商提報，由資安廠商協助解決及即時進行對服務器之漏洞修補。

(4) 導入進階防禦模組，可攔截郵件中附件及檔案夾帶的零時差惡意程式、APT 攻擊工具、含有文件漏洞的攻擊附件等威脅郵件；同時揭露漏洞編碼、攻擊工具及攻擊族群等資訊。

(5) 未來將持續強化資安防護與建立聯防機制，並培訓優質資安人才。

本公司於第十二屆第十二次(112.12.27)董事會通過依目前資通安全組織成立資安專責主管一名由資訊主管兼任，及一名資安專責人員。

P-DUKE Technology Co., Ltd.
Tel +886-4-2359-0668
Fax +886-4-2359-1338
Email sale@pduke.com
Web www.pduke.com
Add No. 36, 22nd Rd., Taichung Industrial Park,Taichung, Taiwan, R.O.C.




2. 資訊安全政策：

(1) 全體同仁皆遵循公司「資訊管理辦法」之規定辦理，並定期檢視與修正以符合現今資安之規範。

(2) 全體同仁主機，每一小時進行防毒更新、資安人員遇有環境威脅即進行作業系統 Patch 更新，以確保公司主機之安全。

P-DUKE Technology Co., Ltd.
Tel +886-4-2359-0668
Fax +886-4-2359-1338
Email sale@pduke.com
Web www.pduke.com
Add No. 36, 22nd Rd., Taichung Industrial Park,Taichung, Taiwan, R.O.C.

3. 具體管理方案：

考量資安險為新興險種，而理賠鑑識機構仍不明確，且理賠條件無法適用所有資安事件，經評估過後暫不購買資安險；另外不定期進行公司員工資安宣導或教育訓練，以提升員工資安意識，本公司目前管理方式已能有效防護資訊安全，具體管理措施如下表：

資訊安全管理措施

| 類型 | 說明 | 相關作業 |
|---|---|---|
| 權限管理 | 人員帳號、權限管理與系統操作行為之管理措施 | 1. 人員帳號權限管理與審核<br>2. 人員帳號權限定期盤點 |
| 存取管控 | 人員存取內外部系統及資料傳輸管道之控制措施 | 1. 內/外部存取管控措施<br>2. 操作行為軌跡記錄 |
| 外部威脅 | 內部潛在弱點、中毒管道與防護措施 | 1. 主機/電腦弱點檢測及更新措施<br>2. 病毒防護與惡意程式檢測 |
| 系統可用性 | 系統可用狀態與服務中斷時之處置措施 | 1. 系統/網路可用狀態監控及通報機制<br>2. 服務中斷之應變措施<br>3. 資訊備份措施、本/異地備份機制<br>4. 定期災害復原演練 |