資訊安全政策及管理方案

為強化資訊安全管理，確保資訊的可用性、完整性以及機密性，並免於遭受內、外部的蓄意或意外的威脅，中國探針資訊安全政策與管理方式分為七大項：

一、電腦設備安全管理

1.本公司各應用伺服器等設備均設置於資訊機房，機房門禁採用感應刷卡進出，且保留進出紀錄存查以及進出需填寫機房進出登記表。

2.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以及 CO2 海龍滅火器可適用於一般或電器所引起的火災，並設置環控系統做為監控。

3.機房主機配置不斷電與穩壓設備，並連結公司大樓自備的發電機供電系統，避免台電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。

二、網路安全管理

1.與外界網路連線的入口，配置企業級防火牆，阻擋駭客非法入侵。

2.台北總公司與各分公司 site to site 的連線作業，使用資料加密的方式，避免資料傳輸過程遭受非法擷取。

3.配置上網行為管理與過濾軟體及硬體，控管網際網路的存取，並禁止訪問釣魚網站或政策不允許的網路位址，強化網路安全並防止頻寬資源被不當占用。

4.加入中華電信資安艦隊包含 IPS 弱點掃描、抵禦 DDOS 攻擊

三、病毒防護與管理

1.伺服器與同仁終端電腦設備內均安裝有端點防護軟體，病毒碼採自動更新方式，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。

2.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使用者端個人電腦。

四、系統存取控制。

1.同仁對各應用系統的使用，透過公司內部規定的系統權限申請程序，經權責主管核准後，由資訊室建立系統帳號，並經各系統管理員依所申請的功能權限做授權方得存取。

2.帳號的密碼設置，規定適當的強度，並且必須文數字、特殊符號混雜，才能通過。

3.同仁辦理離(休)職手續時，進行各系統帳號的刪除作業。

五、確保系統的永續運作。

1.系統備份：建置備份管理系統，採取日備份機制，備份媒體共有兩份，一份保留於機房，另一分廠區(異地)。

2. 災害復原演練：各系統每年實施一次演練，選定還原日期基準點後，由備份軟體還原於異機，再由使用單位測試確認回復資料的正確性，確保備份媒體的正確性與有效性。

3. 租用電信公司兩條數據線路，透過頻寬管理設備，兩線路並聯互為備援使用，確保網路通訊不中斷。

六、資安宣導與教育訓練

1. 定期宣導。每季要求同仁定期更換系統密碼，以維帳號安全。

2. 講座宣導。不定期對內部同仁實施資訊安全相關的教育訓練課程以及觀念落實。

七、成立資訊安全管理組織