資訊安全風險管理架構

集團信息安全委員會負責審查各子公司的安全政策，監督本集團安全管理的運作，並定期向高層會報告安全的管理；安全控制結構包括協助各點和保持集團安全性，每個點都有自己的本地安全控制，主要控制機房為深圳，由信息安全委員會負責監督和管理整個集團的安全控管，安全風險管 理涵蓋各種範圍，如資料、資料庫、應用程式、可存取性、安全性。

資訊安全政策

安全策略的主要目標是關注安全管理，法律合規和技術應用三個方面，從系統到技術， 從人員到組織，全面提高安全防護能力。

鑑於當前資產安全的新趨勢，如勒索軟件，社交工程攻擊和虛假網站，我們定期由信息安全委員關注安全問題和規劃。針對該計劃，對不同的安全場景進行了攻防演練，加強處理人員的彈性，以便在第一時間檢測並完成防堵，此外也經常進行培訓和課程。所有的用戶都被要求參加。

安具體的管理計畫

為了防止將資訊錯誤發送到外部電子郵件地址或外部連接到我們的網絡, 我們會屏蔽並 限制具有潛在風險域的進出,至少包含下列項目：

1.定期對安全管理員進行培訓

2.行動設備安全控制包括消除和刪除設備資料

3.資料遺失防護端點 - 設備可存取性的控制

4.可疑登錄和從多重設備登錄的警報

5.網絡釣魚和惡意軟件防護

6.災難恢復

7.定期安全檢查 (1)多個設備連接 (2)設備位置(3)兩步驗證

8.密碼強度和長度的強制和監控

9.多層登錄驗證

10.電子郵件 TLS 安全加密

所有員工均定期參加培訓，以進一步提高資訊安全意識。為業務合作夥伴進行資訊安全宣傳資訊洩漏的風險程度到達了前所未有的高度。為了能彈性應對此問題，集團實施了資料遺失的預防和加密。