欣高石油氣股份有限公司資通安全管控辦法

第一章 總則

第一條、 為強化本公司資通安全防護與管理，訂定本(以下簡稱資通安全)辦法。

第二條、 管理範圍:

一、 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、 資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

核心業務：業務部用戶裝置申請、掛表申請資料之建置及存取，財務部記帳憑證及財務相關報表之存取，管理部人事資料之存取，工務部供氣系統、圖資系統、工程設計及估價系統之建置及存取，應維持正常運作與繼續發展業務之功能。

三、 核心資通系統：支持核心業務持續運作必要之資通系統建置如需外包，則依本公司採購辦法執行。

四、 機密性資料：依公司業務認定，各部門提共資料由資安主管評估保密層級，機密資料存取由總經理核決。

第二章 資通安全政策推動組織

第三條、 成立資通安全推動組織，配置資安主管 1 位及資安人員 1 位，以負責推動、協調監督及審查資通安全管理事項。

第四條、 資通安全政策及目標由總經理核定，並定期檢視政策及目標可以有效傳達員工知其重要性。

第五條、訂定資通安全作業程序，包含核心業務及其重要性、資通系統盤點及風險評估、資通系統發展及維護安全、資通安全防護及控制措施、資通系統或資通服務委外辦理之管理措施。

第六條、 公司全體員工每年接受資訊安全宣導課程，另負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練。

第三章 核心業務及其重要性

第七條、 部門主管應鑑別所承辦業務是否符合機密性質，由資安主管判定之後列入機密檔案，資安主管應定期檢視公司之核心業務及應保護之機密性資料，機密資料存取由總經理核定。

第八條、 員工應遵循個人資料保護法、部門作業程序之規範，及資通安全宣導之要求。

第九條、 年度結束後於次年 1 月 31 日之前，資安主管應鑑別可能造成營運中斷事件之發生機率及影響程度，訂定預期性改善計畫並出據報告。資料應備份並易地保存，保存方式應另機、另地存放。

每年排定資安宣導至少 1 次，由全體員工參加，宣導內容應含資安之重要性、資安法令、電腦存取應注意事項，探討國、內外發生之資安事件。每年檢視核心業務持續運作能檢查，內容包含業務部門用戶個資及財務部會計系統運作，管理部員工個人資料系統、出納人員網路銀行及 ACH 付款系統之安全性，及工務部管線設備、安全維護系統、電子郵件與外部連結網站之使用，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。

第十條、 每年檢視備援措施、人員職責、資源運用是否足以因應資訊安全功能，檢視結果應作成報告。

第四章 資通系統盤點及風險評估

第十一條、定期盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值。

第十二條、每年辦理機房環境安全評估及檢查有無外力入侵之可能性。

第五章 資通系統發展及維護安全

第十三條、軟硬體採購及資安設備採購悉依本公司採購辦法辦理，程序為:需求簽核，經核決權人核准之後招商、估價及報價。機密資料應以承辦人員身分證字號為設定密碼，存取控制經承辦人向資安主管提出

申請，由總經理核決。

第十四條、每半年檢查機密資料存取之安全性，使用者登入之身分驗證及使用者輸入輸出檢查過濾測試，如發現有未經核決進入機密資料庫存取，應立即檢視入侵原因。

第十五條、妥善儲存管理資通系統開發商及維護合約相關文件，包含程式紀錄及盤點功能、程式開發供應商之保密承諾、程式專利權歸屬。

第十六條、對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。

一、 定期辦理弱點掃描。

二、 定期辦理滲透測試。

三、 系統上線前執行源碼掃描安全檢測。

第六章 資通安全防護及控制措施

第十七條、公司設立內網路及外部信箱應僅限公司專用網站，不得連結私人帳戶，收發也應限於公務相關之業務。

第十八條、具備下列資安防護控制措施：

一、 防毒軟體。

二、 網路防火牆。

三、 如有郵件伺服器者，具備電子郵件過濾機制。

四、 入侵偵測及防禦機制。

五、 如有對外服務之核心資通系統者，具備應用程式防火牆。

六、 進階持續性威脅攻擊防禦措施。

七、 資通安全威脅偵測管理機制(SOC)。

第十九條、針對機密文件應存放於專用電腦並予以加密，由專人專區保管，保管人員資格應具工作年資達 10 年以上。

第二十條、員工到職、在職及離職管理程序依據本公司人事規章辦理，全體員工應簽署保密協議。

第二十一條、 管理部出納 ACH 系統係外部程式，應三個月變更一次密碼，資金放行或轉帳應設 2 層放行密碼，第一層為財務經理，第二層為總經理。

第二十二條、 定期審查特權帳號、使用者帳號及權限，停用 1 年未使用之帳號應由資安主管會同承辦人取消帳號及權限，並經總經理核決。

第二十三條、 電腦機房入口及內部應裝置攝影機，以監控機房設備之安全性，設置登記簿供進出電腦機房人員(含外包廠商)登記，機房應上鎖，鑰匙由資訊室主管及其代理人各持 1 把，裝置適當的冷氣設備及除濕設備。

第二十四條、 留意安全漏洞通告，即時修補高風險漏洞，定期評估辦理設備、系統元件、資料庫系統及軟體之安全性漏洞修補。

第二十五條、 資通設備汰除應先簽核，會同管理部資產管理承辦人以破壞性之方式破壞銷毀，並確定機密性資料已刪除。

電腦裝置使用管理規範；不得安裝未經許可之軟體、電子信箱僅供收發與業務有關之信件、應避免個人行動裝置及可攜式媒體裝置。

第二十六條、 委外廠商之資通安全責任及保密規定，於採購文件或合約中載明服務協議、資安要求及對委外廠商資安稽核權。

第二十七條、 合約應訂明委外關係終止或解除時，廠商應返還、移交、刪除或銷毀履行契約持有之資料。

第七章 資通安全事件通報應變及情資評估因應

第二十八條、 資安事件發生應立即依據「資安事件通報作業流程圖」(附圖 1)」通報，並依據「資安事件應變作業流程」(附圖 2)辦理。

第二十九條、 發生重大資安事件依「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序」申報及公告。

第三十條、資通安全推行於年度結束次年 1 月底，向管理階層報告資通安全執行情形，確保運作適切性及有效性。

第八章 附則

第三十一條、 本辦法經董事長核決通過後實施，修訂時亦同。