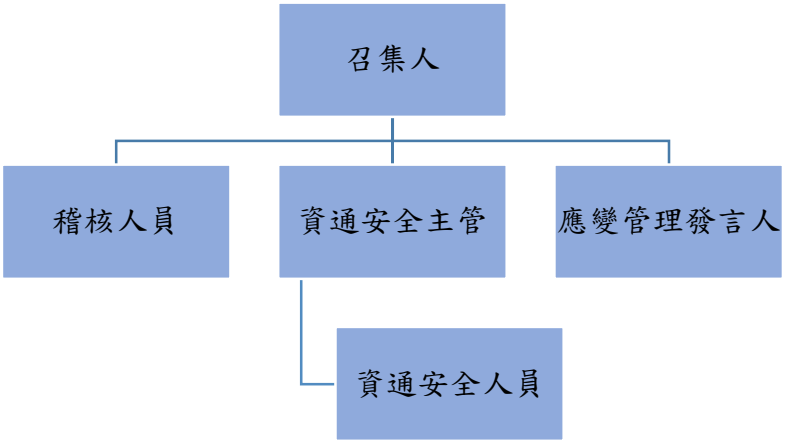
金洲海洋科技股份有限公司
資通安全政策及具體管理方案



- 本公司「資通安全推動小組」，由總經理擔任召集人，設置應變管理發言人、稽核人員、資通安全主管及資通安全人員各一名。
- 資通安全推動小組負責規劃暨執行資通安全政策，並定期向董事長報告公司資通安全治理概況。
- 資通安全推動小組每年定期召開 「資通安全管理會議」，檢討資通安全相關議題，以利了解公司資通安全治理概況。113 年召開 1 次。
- 資通安全人員通過經濟部產業人才「中級資通安全工程師」能力鑑定。
- 本公司訂有「資通安全作業程序」及「核心業務持續運作計畫」。
- 資通安全人員每年依據「資訊資通資產盤點及風險評估表」盤點資訊資通資產及評估風險，由稽核人員查核盤點結果，根據盤點及風險評估結果製作計劃書與具體因應作為，並定期追蹤改善成效，以降低內部資通安全風險。
- 本公司每年針對重要作業系統演練災難復原，確保發生災難時，能以最短的時間回復正常。
- 本公司已加入「台灣電腦網路危機處理暨協調中心」，以獲取最新資通安全情報。

【資通安全政策】

為強化資訊安全管理，確保資訊的機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），並免於遭受內、外部的蓄意或意外的威脅，資訊安全設施與管理方式分為六大項，茲闡述如下：

一、電腦設備安全管理

1. 本公司電腦主機、各應用伺服器等設備均設置於專用機房，且進出保留紀錄存查。

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，可適用於一般或電器所引起的火災。

3. 機房主機配置不斷電與穩壓設備，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. 台灣總公司與各國分公司、工廠據點 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設備，控管網際網路的存取，可屏蔽訪問有害或政策不允許的網路位址與內容，強化網路安全並防止頻寬資源被不當占用。

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的 PC。

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電子簽核申請程序，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，並且必須英文、數字、特殊符號混雜，才能通過。

3. 同仁辦理離(休)職手續時，若為辦公室相關人員，必須會辦資訊室，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，另一份備份媒體存放於銀行保險箱(異地)。

2. 災害復原演練：每年實施一次演練，選定還原日期基準點後，由備份媒體回存於備份系統主機，再由使用單位同仁確認回復資料的可靠性，再由資訊人員確認資料的正確性，確保備份媒體的有效性。

3. 租用電信公司多條數據線路，透過頻寬管理設備，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，以維護帳號安全。

2. 通訊軟體通知: 若有相關的資訊重要訊息，會以 Email 或 通訊軟體群組 來通知。

3. 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。