羅 麗 芬 控 股 股 份 有 限 公 司
L U O L I H - F E N H O L D I N G C O . , L T D .
2 0 2 4 年 度 資 通 安 全 風 險 管 理 及 執 行 情 形 報 告

本公司自成立之初即設立資訊課，負責公司資訊系統建設與資訊安全，歷經多年發展資訊課已發展成為資訊部，並設立資訊部經理一職直接領導，由總經理分管，同時總經理作為資訊安全管理者代表，負責資訊安全的綱領性指導。本公司按照 GB/T 22080-2016 /ISO/IEC 27001:2013 建立資訊安全管理體系，並已取得資訊安全管理體系認證(有效期為 2024/01/22-2027/02/21)，全面保護本公司的資訊安全。本公司 2024 年度資通安全風險管理及執行情形如下:

一、資通安全政策

本公司資訊安全方針為：實施風險管理，確保資訊安全，保障業務可持續發展。

1.實施風險管理：

根據本公司業務資訊安全的特點、法律法規要求，建立風險評估程式，確定風險接受準則。定期進行風險評估，以識別本公司風險的變化。本公司或環境發生重大變化時，隨時評估。應根據風險評估的結果，採取相應措施，降低風險。

2.確保資訊安全：

在日常企業生產和管理中，對資訊安全予以重視，全面識別和分析全部資訊資產，系統考慮企業資訊系統薄弱點、可能存在的威脅、考慮成本、利益、風險的綜合平衡，對資產進行分類保護，以適宜的成本達到系統保護的要求。

3.保障業務可持續發展：

建立健全資訊安全監督和保證體系，明確各級、各崗位的資訊安全責任，以人為本，堅持全員、全方位、全過程資訊安全管理。通過測量和監控，持續改進，保證資訊安全管理體系的有效運行，做到制度執行有記錄、記錄記載可追溯，最終保障企業生產、經營、管理和服務的持續和安全，實現企業發展目標。

二、具體管理方案及投入資通安全管理之資源

為建設符合管理措施的資訊安全企業，本公司還投入了相應的設備和系統如防火牆系統、行為管理系統、備份一體機、共用許可權管理、加密軟體等，更好的完善了資訊安全管理方案的實施，以下為各項設備和系統的功能介紹：

1.防範來自於網路外部的威脅—防火牆：

在網路安全事件中，資訊安全攻擊大部分來自於網路。其中包括 DDOS 拒絕服務式攻擊、ARP 攻擊、TCP/UDP 攻擊、埠掃描等攻擊手段。本公司配備了 AF-1210 型號的防火牆，具有良好的網路安全防護功能，可以對以上提到的各種攻擊手段起到良好的防護作用。

2.防範來自於網路內部的威脅—行為管理：

對於內部網路的安全管控，本公司啟用了上網行為管理系統，對於網路使用者只啟用足夠使用的網路許可權，有效的防止了內部使用者訪問病毒網站、釣魚網站，阻斷了不良網站可能存在的危險行為。

3.保護資料的安全—備份一體機：

資料是企業生存的命脈，是資訊安全工作的重點。為了保證資料安全，本公司資訊安全部門引進了備份一體機系統，用於對企業的各項業務持續進行備份，以備在發生資訊安全問題時能夠在第一時間恢復資料，同時備份資料也可以讓資料損失達到最小化。

4.資料安全互通—共用許可權管理：

共用許可權管理為公司資料提供了一個平臺，所有的資料都可以通過共用來實現資料互訪，並且共用許可權管理平臺還可以針對個人設置不同的存取權限，保證資料安全。

5.減少洩密風險—加密軟體：

本公司不僅在各個途徑實現了對資料和網路的管控，還對資料本身的安全性提出了更高的要求，加密軟體的引進就是這一思想的直接成果。通過加密軟體我們可以把資料即時加密，從源頭上防範了資訊洩露，只有通過加密軟體才可以把資料解密出來，沒有安裝加密軟體人員無法識別加密後的檔，減少了資訊洩露的風險。

三、2024 年度執行情形:

1.資訊部 2024 年度已完成 361 人次資訊安全宣導及案例宣傳，另外每年結合國家網路安全宣傳周會做專門培訓學習。

2.為了確保各部門資料的安全性，資訊部增加一台檔共用存儲，實現原有共用管理平臺主從備份管理。進一步加強各部門資料安全和確保因硬體問題可以實現快速切換運行。

3.為了進一步確保公司資料安全，對公司所有 PC 進行 USB 管控，所有接入公司 U 盤或移動硬碟必須經過領導審批後，由資訊部進行認證後才可以在規定的 PC 上使用。未經認證的 U 盤、移動硬碟都無法識別使用。

4.資訊部 2024 年度根據年度計畫對公司的資訊安全進行 7 次演練測試並形成演練報告。

5.根據資訊安全管理體系相關制度內部審核員根據計畫對各部門資訊安全列為審核專案，並將審核結果呈報給體系小組進行跟蹤檢查需整改專案。