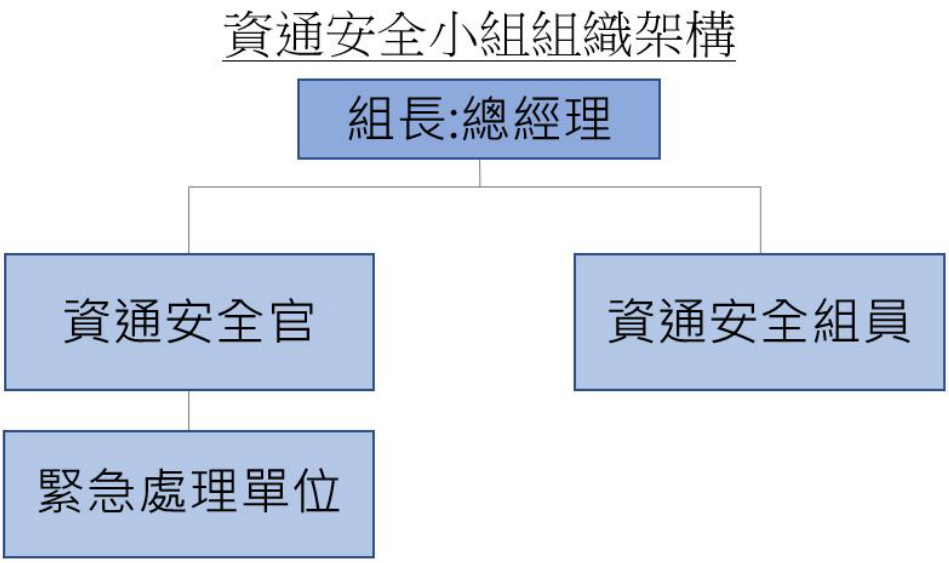
竹陞科技股份有限公司

資訊安全政策

一、建置資訊安全風險管理架構

成立資通安全小組，定期檢討資安政策，並定期向董事會報告。

資通安全小組組織架構:



1. 組長:

   由總經理擔任招集人，能夠確保整個組織對於資訊安全的重要性有足夠的認識，並提供必要的資源和支持。

2. 資通安全官:

   由資訊部人員擔任，負責制定和推動資訊安全政策，確保整體資訊安全策略的實施，同時也是提升員工資安意識的推動者。

3. 資通安全組員:

   由各一級主管組成，負責執行各項資訊安全措施，例如: 監控系統漏洞、執行安全訓練、確保遵循安全政策等。

4. 緊急處理單位:

   應對非預期資訊安全事件，快速制定應急措施以減少損失。

二、資訊安全政策與具體管理方案

資訊安全政策

1. 建立資訊資產監控及管控機制，所有人員均有責任及義務保護其所負責之相關資訊資產，以確保本公司重要資訊資產之機密性、正確性及可用性。
2. 確保員工的工作職掌得到適當劃分，并僅賦予他們完成工作所需的必要權

限和資訊。

3. 錄用新員工時，必須進行適當的考核，並要求他們簽署相關的工作規範，以使每個員工了解維護和確保資訊安全是他們的義務，落實於日常工作中。
4. 建立業務持續運作管理機制，以確保其始終保持適用性。
5. 本公司的資訊安全措施必須遵守法律規定和公司的資訊安全政策要求。建立和修改所有資訊安全規範或程序時，必須遵守和遵循資訊安全管理體系的機制。
6. 積極確保內部資料的保護、保存和安全，以防止不當和非法行為。
7. 當資訊安全事件發生導致權益損害時，必須立即進行適當的回應與處理。

具體管理措施

網際網路資安管控	**權限及資料存取管控**	**應變復原機制**	**資安宣導**
1. 架設網路防火牆並定期檢查韌體更新 2. 防毒軟體定期對電腦系統及資料儲存媒體進行病毒掃瞄 3. 各項網路服務之使用應依據資訊安全政策執行 4. 每日檢查各項網路服務監控系統之 System Log，若發現異常情況，應當紀錄於電腦機房異常紀錄 5. 定期維護公司網站資安漏洞	1. 電腦設備應有專人保管，並設定帳號與密碼 2. 依據職能分別賦予不同存取權限 3. 調離人員取消原有權限 4. 設備報廢前經相關主管簽呈同意，先將機密性、敏感性資料及版權軟體移除或覆寫 5. 遠端登入管理資訊系統經相關主管簽核同意，適當之核准 6. 當同仁欲使用資料儲存媒體時，必須經相關主管簽核同	1. 定期檢視緊急應變計劃 2. 每年定期演練系統復原 3. 建立系統備份機制，落實異地備份 4. 定期檢討電腦網路安全控制措施	1. 定期宣導資訊安全資訊，提升員工資安意識

	意，使得授予存取權限 7. 機房出入權限管制		

三、投入資通安全之資源及執行情形

1. 本公司為了保護公司重要檔案資訊，有別於一般文件保護，投入 D-Security(以柔)原始檔案保護系統對導入保護的衝擊與管制並重，針對文件自企業內部提出申請外發保護，可由內部流程審核確認管制功能，通過審核後即可轉換為外發檔案提供給外部。
2. 外部人員接收檔案時使用即會受到唯讀、開啟密碼、內容防護、列印、截圖等管制，讓檔案外發後仍可在管制下運作，達到安全分享的效果。
3. 於建置電腦機房設立門禁系統，僅資訊人員有權限進入機房，設立機房溫溼度監測、保護公司系統重要設備。
4. 使用鼎新系統 ERP 整合為兩岸三地企業資訊，提供財務、庫房、訂單資訊透明化、並節省紙本進行電子化簽核，也每日做到重要檔案的異地備援建置。
5. 機房設備受到 UPS(不斷電系統)保護，以防止跳電和停電的影響，並降低資料損失的風險，與 UPS 廠商簽訂 UPS 定期保養合約，以確保設備在需要時能夠正常運作，並保障機房的資訊系統運行的可靠性和穩定性。

112 年度資通安全管理執行情形如下:

1. 資訊安全宣導:每季發布 1 次資安宣導，同仁回覆率 100%。
2. 資安事件處理:發生資安事件 1 次，資訊安全單位持續稽核，確保資通環境安全。
3. 資通安全小組報告:每年召開 1 次