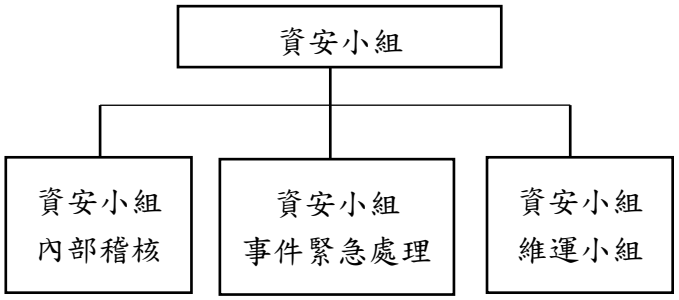
中化合成生技股份有限公司
資通安全風險管理架構

本公司已訂定電腦化資訊系統管理制度作業辦法及資通安全作業程序，以落實內控制度與維護資通安全政策。透過每年內部檢視和外部評估其安全規章及程序，確保其適當性和有效性。以下分項進行詳細說明：

(1)資通安全風險管理架構：



本公司於資訊部下成立資安小組，組織如上圖，由資訊部主管擔任資訊安全專責主管，並配置資訊安全專責人員一名，負責制定資通安全政策並定期檢討修正及資訊制度規畫、監控及執行資訊安全維護作業。每年定期由稽核室及會計師事務所執行內部稽核及外部查核，113 年 4 月稽核室執行資通安全檢查控制作業之內部稽核，並出具內部稽核報告，呈報審計委員會及董事會，並於 113 年 11 月經資誠聯合會計師事務所執行「資訊系統環境查核」之外部查核。系統所用的伺服器主機，皆位於內部虛擬網路之中，透過防火牆保護內部主機，外部網路受隔離無法直接進入，並已採用多重網路安全防禦系統，位於網路前端之防火牆、入侵偵測系統、防毒做為企業資安防護基礎外，並可針對流量、網頁與郵件，加強惡意程式的偵測，藉由不同安全機制的關連分析，發揮縱深防禦的功效，並即時封鎖最新惡意軟體，有害之網站連結，防禦外部網路攻擊、郵件內容安全控管系統負責過濾信件進出連線的內容，可進階攔截檔案夾帶零時差(Zero-day)惡意程式、APT 攻擊工具、含有漏洞的攻擊文件…等威脅郵件、垃圾電子郵件之威脅。位於內部之主機及端點皆由中控台佈署防毒軟體，隨時更新病毒碼與即時辨識惡意行為特徵，能即時攔截病毒木馬蠕蟲、勒索軟體、文件夾帶之惡意程式等，有效降低被駭客攻擊損害之風險。

(2)資通安全政策：

為使本公司業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），制訂資通安全政策如下：

A.定期實施資通安全教育訓練，宣導資通安全政策及相關實施規定，推廣員工資通安全之意識與強化其對相關責任之認知。

B.實施資通安全內部稽核制度，確保資通安全管理之落實執行。

C.保護本公司業務活動資訊，避免未經授權的修改，確保其正確完整性，保護本公司資料、系統、設備及網路通訊安全，阻絕外界之入侵及破壞。

D.保護本公司業務活動資訊，避免未經授權的存取，系統資訊帳號存取權限與系統之變更，均都須經過權限控管。

E.保護公司資料完整性，落實銷毀程序，已報廢之電腦儲存媒體應加以銷毀避免資料

意外暴露外流。

F.監控資訊系統之安全狀態與活動紀錄，有效掌握並處理資通安全事件。

G.本公司之業務活動執行須符合相關法令或法規之要求。

目前本公司資通安全維護措施完備，考量資安險仍是新興險種，因涉及資安分級和理賠鑑識等配套，故尚在評估未來適用性之階段。

(3)資通安全具體管理方案：

A.系統帳號與權限管理

電腦化系統應有充分權限管制，以防止未經授權的侵入或使用者擅自對資料進行變更，內容包含資通安全權責、資訊存取權限及資訊存取控制，可依電腦化系統的重要性，來決定安全控管的程度。使用者之帳號及權限，資料之存取皆需經權責主管核准後始能使用與變更。離職人員（含留職人員）應依處理程序立即鎖定、停止或移除帳號及權限，以防範未經授權之使用。

B.資料存取紀錄稽核備存

本公司為確保資料完整性，電腦化系統應當能記錄異動歷程，即任何資料的變更/刪除、由誰進行、能紀錄系統檔案文件存取之軌跡記錄、有關往來郵件等歷史資料，進行歸檔保存。報廢程序完成之電腦均執行硬碟拆解破壞以符合法規遵循的管理制度及資安政策。

C.資訊系統持續運作

確保本公司資料、系統、設備及網路通訊安全，建立資料/備份的方法及備援作業標準書，系統與文件皆採取每日、每週及每季之本地備份，每日、週、季之備份資料再傳輸到異機或存放到異地做為異地、異機備份，加強機房各項模擬測試與緊急應變等演練以確保資訊系統之正常運作及資料保全。每年定期執行系統資料復原測試演練，以確保資訊系統之正當運作及資料保全，可降低無預警天災及人為災害造成之資料損失風險。113 年 5 月已執行 IT 災害復原(ITDR)演練測試，本公司資訊系統持續有效運作，無重大資料損失風險。

(4)投入資通安全管理之資源：

本公司資訊部主管擔任資訊安全專責主管，並配置資訊安全專責人員一名，負責資訊制度規畫、監控及執行資訊安全維護作業。本公司不定期以時事案例透過公司內部網路對員工做資通安全宣導，傳達資安防護重要規定與注意事項。為強化本公司資訊安全技術及安全防護，113 年投入資通安全防護相關費用共計 646 仟元，每年定期向董事會報告資通安全管理及執行情形。

113 年投入資通安全防護相關費用：

<table>
<tr><th>訓練/購置</th><th>參加人數</th><th>每人訓練時數</th><th>總費用
(新台幣仟元)</th></tr>
<tr><td rowspan="2">年度郵件社交工程演練暨資訊安全教育訓練</td><td>36</td><td>1</td><td rowspan="4">646</td></tr>
<tr><td>16</td><td>2</td></tr>
<tr><td>外部訓練課程:資安弱點與源碼掃描工具</td><td>2</td><td>7</td></tr>
<tr><td colspan="3">購買資通安全防護軟體</td></tr>
</table>

本公司生產線機台皆獨立作業並未連接網際網路，因此病毒影響造成廠區當機事件的風險相對較低，辦公室每台桌上型電腦及 NB 皆安裝防毒軟體，除了啟用即時掃描功能並定時主動為每台電腦掃毒，且每日更新病毒碼。以及信件接收都經由 SPAM SQR Server 過濾，並增購 SPAM SQR ADM 防禦模組以及 DKIM 簽章，減低社交郵件和釣魚信件風險，定時資安教育訓練，或不定時資安郵件通報，提高人員資安意識風險，公司內部網路連線自建 VPN，並有防火牆防護，阻斷了病毒於廠區內互相感染的風險。透過內部檢視和外部評估其安全規章及程序，資訊部門依照作業執行本公司規定程序均能落實執行，確保公司資料完整性與安全性，風險評估結果尚屬良好，迄今並未發現任何重大的網絡攻擊或事件，對公司業務及營運無重大不利影響。本公司未曾涉入任何與此有關的法律案件或監管調查，科技改變對公司資通安全並無重大不利影響且無重大營運風險。