資通安全管理策略與架構

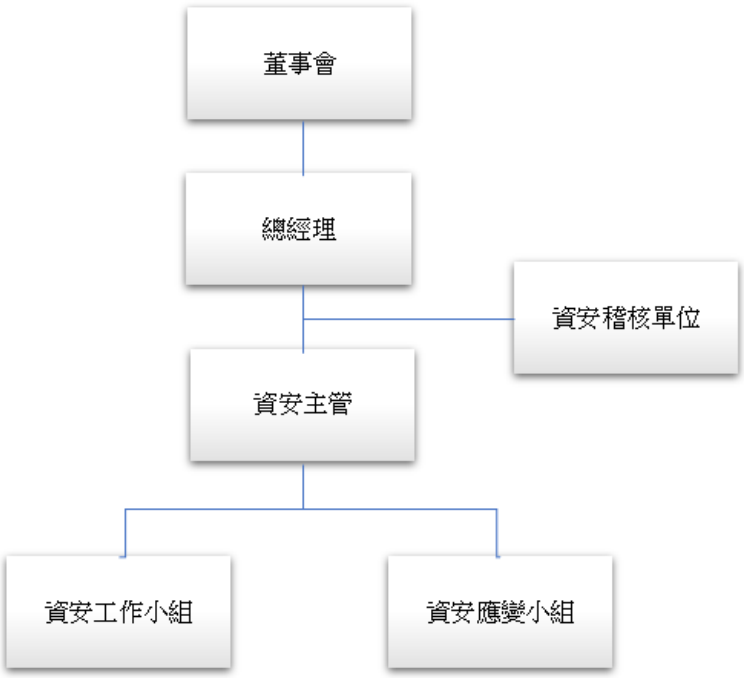
敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。

（一） 資通安全風險管理架構

宏亞食品股份有限公司（以下簡稱本公司）在民國112年設立及申報「資安專責主管」與「資安專責人員」，負責執行資訊作業安全管理規劃，建置與維護資訊安全管理體系，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核。

資安專責主管不定期於內部向總經理及各部主管進行資安工作報告，每年接受資訊安全內部稽核以及外部第三方稽核審查，並因應稽核審查結果採取對應之防護及矯正措施以緩解降低資安風險，確保資訊安全管理體系持續運作的適用性、適切性及有效性。

資安主管於每年向董事會彙報資安管理成效及資安策略方向，並依據領域背景相關之獨立董事所提出相關意見進行檢討修正。



（二） 資通安全政策

宏亞食品股份有限公司依據所辨識之資訊安全風險擬定管理政策(包含遵循標準、

管理及執行)，並依據上述政策發展制定具體管理作業加以落實 (包含安全管理作業、防火牆管理、使用者系統權限管理、資料修改申請管理、資訊系統緊急應變、資訊系統檔案備份管理、資訊設備報廢及交接作業管理及電子檔案管理等)，除了在公司內部正式進行公告及頒佈，並同時納入內部日常控制作業。

本公司的資訊安全政策也同時涵蓋子公司全體同仁，是以:

一、 建立符合法規與客戶需求之資訊安全管理規範。
二、 透過全員認知，達成資訊安全人人有責的共識。
三、 保護公司與客戶資訊的機密性、完整性與可用性。
四、 提供安全的生產環境，確保公司業務之永續營運」為指導準則。
五、 以防毒、防駭、防漏三大資安防護主軸為目標，建立次世代防火牆、IPS入侵偵測系統、WAF、防毒系統及諸多內控系統，以提升公司防禦外部攻擊之能力，並確保內部重要資訊之防護。

（三） 具體管理方案

為達資安政策與目標，建立全面性的資安防護，本公司資安工作的具體管理除遵循ISO 27001指引及控制措施，同時也參照國際著名資安管理框架NIST CSF，以建立多層次縱深防禦能力:

一、 多層次防護體系

- 網路安全:佈署建置次世代防火牆(NGFW)暨整合UTM統一威脅管理，應對現代新型態資安攻擊與威脅。另外，針對無線設備導入IEEE 802.1X安全管控，所有IT設備連線須以AD帳號進行身份驗證、OT設備以MAC驗證控管連線存取。外部VPN連線導入MFA多因子身份安全驗證機制，大幅強化連線安全。公司相關對外網站導入TLS加密憑證，確認資料傳輸安全。
- 端點安全:所有端點安裝防毒軟體，並每週強制進行系統scan掃瞄。電腦OS須升級到合規版本，並持續接收WSUS伺服器之security patch更新修補。
- 郵件安全:電子郵件透過公司Exchange Server收發，並建置郵件防火牆進行防護與內容過濾管控，同時建置郵件歸檔系統以確保郵件軌跡可追蹤追溯。另外，亦不定期進行郵件社交工程演練，強化同仁郵件資安防護意識。
- 帳號安全:盤點重要之系統特權帳號並特別進行管制，相關帳密資訊所存放之文檔予以加密保護 ； 全體同仁AD帳號密碼及重要系統帳密(e.g. ERP系統)強制定期變更，密碼設定必須符合一定的強度規範 ； 盤點所有

IT及OT連線設備帳密，確保所有設備未使用出廠預設密碼。

- 資料安全:依照部門及使用者職務進行適切之存取權限設置，對於公司資料妥善建立本地備份、異地備援、災難復原計劃及演練。同時，為了有效抵禦勒索病毒之攻擊危害風險，針對資料進行離線備份以及加密備份，確保所有備份資料能夠還原使用。

二、 提升員工資安意識與風險認知

- 不定期以e-mail發送資訊安全公告給全體同仁。
- 每年不定期於全體員工會議進行資訊安全宣導。
- 不定期安排資安工作執行同仁參加外部專業課程及研討會。
- 每年邀請專業資安廠商到公司進行資安教育講座。
- 每年透過專業資安廠商至少執行2~3次郵件社交工程實務演練。

三、 持續監控及改善

- 弱點掃瞄:不定期委託第三方資安專業廠商，進行主機與網站弱點掃瞄並執行漏洞修補。另外，針對委外供應商所開發之網頁程式也進行弱掃，確認廠商程式無資安漏洞、確保供應鏈資訊安全。
- 資安健診:不定期委託第三方資安專業廠商，主動尋找伺服器、個人電腦、防火牆等之錯誤組態設定 / 惡意程式活動 / 異常連線行為，健診後進行修正並消除相關風險威脅。
- 持續透過資安教育訓練、資安宣導、社交工程演練等活動來強化同仁資安認知，並經由監控同仁進行電腦高風險操作行為之狀況及統計數據，以確認同仁們的資安意識能保持穩定提升進步。

另外，為達到資安聯防的效果，本公司已於民國111年完成加入TWCERT/CC(台灣電腦網路危機處理暨協調中心)，進行資安情資共享、威脅預警、聯防。

同時，本公司之主要資訊設備及資料放置於宏遠電信機房，此IDC機房已通過"個人資料保護法 PIMS ISO29100認證”及"資訊安全管理系統 ISMS ISO27001認證”。

（四） 投入資通安全管理之資源

資訊安全為本公司營運之重要議題，對應資安管理事項及投入之資源方案如下：

一、 個人電腦作業系統升級:投入人力及資金進行全公司電腦暨作業系統升級，符合安全合規之電腦升級比率(微軟Win 10 22H2以上版本比例)已達到95%以上。

二、 資安弱點掃瞄:委託專業資安廠商進行主機與網站資安弱點掃瞄，並進行漏洞修補，以民國112年為例，年底進行的掃瞄與年初相較，高風險漏洞修補率

已達到90%以上。

三、 資安健診:委由第三方專業資安廠商進行全公司資訊環境資安健診，以民國112年為例，年初健診後所發現之Critical/High風險數各為260/622個，於同年底之前已100%完成修補矯正。

四、 客戶滿意：無重大資安事件，無違反客戶資料遺失之事件發生。

五、 一般員工教育訓練：所有新進員工到職後皆完成資訊安全教育宣導課程；全體員工接受資安教育訓練及宣導，以民國112年為例，共舉辦五次訓練宣導活動。

六、 資安人員教育訓練:安排本公司資安專業人員不定期參加專業訓練課程，以民國112年為例，共計參加四門專業資安課程，累計達152個訓練時數。

七、 社交工程演練:每年執行社交工程演練，以民國112年為例，全年度共計執行三次模擬演練，每次以2~3封測試郵件進行。

八、 資安公告：不定期以電子郵件進行全公司資安宣導公告，傳達資安防護重要規定與注意事項，平均每季公告一次。

九、 供應鏈：本公司之外包資訊廠商所承接開發之網頁程式需接受弱點掃瞄工具檢測，並依風險評等結果執行弱點修補及接受弱掃複測。

十、 認證：本公司主要資訊設備及資料儲存colocation於宏遠電信機房，該IDC機房已通過"個人資料保護法 PIMS ISO29100認證”及"資訊安全管理系統 ISMS ISO27001認證”。