文件編號 ：2A028
建立日期:111/8/2
修訂日期:111/8/2

宏亞食品資訊安全政策

資訊安全組織

本公司成立資訊安全管理團隊，由資訊部最高主管擔任召集人，並由實際執行資訊安全計畫之網路服務成員共同組成。團隊負責外部資訊風險評估與資源導入協助、資訊安全制度建置、資訊安全督導、持續強化資訊安全方面觀念。

制定目的

宏亞食品股份有限公司（以下簡稱本公司）為維護整體資訊安全，強化各項資訊資產之安全管理，確保其具機密性、完整性、可用性，並建立安全及可信賴之作業環境，確保資料安全、系統安全、設備安全、網路安全，保障本公司同仁與相關內部人員與外部人員之權益，特訂定本政策。

範圍

本政策適用於本公司各單位之全體同仁、委外廠商、外部資訊服務(包含雲端服務)第三方人員及所有相關資訊產品，為避免因人為疏失、蓄意或是天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，因而造成本公司各種可能之風險災害。

宏亞食品資訊安全執行情形

宏亞食品已經成立資訊安全組織，設定嚴謹的資訊安全布局與完善的資訊安全管理流程，並由資訊部主管向總經理報告資訊安全執行成果、政策執行狀況與未來規劃，共包含四大主題。

(一) 企業常見的資訊安全攻擊及威脅

(二) 宏亞食品資訊安全策略

(三) 提升同仁資訊安全意識

(四) 強化資訊安全基礎建設

本公司訂定資安政策目標為確保資訊的機密性、完整性和可用性

(一)可用性 - Availability：

確保各項資訊資產能提供即時且正確的服務，以滿足使用者之需求。

(二)完整性 - Integrity：

將資訊資產依重要性分類，並提供適當的保護以確保資訊資產的完整性。

(三)機密性 - Confidentiality：

適當的劃分資料的機密等級，並依其機密等級予以適當的規範及保護。

本公司資訊安全遵循標準為 ISO27001，但本公司非依規定對資訊安全政策及具體管理方案取得國際認證要求之公司，本公司將持續強化資訊安全防護與建立聯防計畫，除此之外，並由小組人員每年度持續參與資訊安全管理相關進修課程，以提昇專業職能並掌握關注議題。

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

文件編號 ：2A028
建立日期:111/8/2
修訂日期:111/8/2

資訊安全政策具體管理方案與執行狀態

一. 人員安全管理及教育訓練

作業:

持續建立、宣導及推廣員工資訊安全認知，以提升資訊安全水準

執行狀態:

1. 不定期使用 E-Mail 發送資訊安全公告
3. 公司同仁每年執行資訊安全宣導
4. 不定期社交工程郵件演練

二. 電腦系統安全管理

作業:

安全管理、 異動管理、使用管理、委外管理

執行狀態:

1. 公司電腦一律安裝商業防毒軟體，且啟動自動更新
2. 公司電腦作業系統需要保持最新狀態，並啟動自動更新
3. 重要資訊系統異動依照軟體管理進行更新作業
4. 委外廠商維護管理作業需依據申請單申請後進行作業

三. 網路安全管理

作業:

外部連線管理、內部連線管理

執行狀態:

1. 網際網路連線管理 (防火牆架設)
2. 公司內網切分不同 V-Lan 及網段進行管理

四. 系統存取控制

作業:

系統存取政策、人員異動管理、人員識別管理、遠端存取管理

執行狀態:

1. 系統存取權限按照職位與部門分別設定
2. 人員異動與權限變更需要按照執行流程留下紀錄
3. 居家辦公或是外勤同仁連回公司一律使用 VPN 軟體經過資訊加密安全通道連線

五. 系統發展及維護安全管理

作業:

系統開發管理、委外廠商管理、委託期間管理

執行狀態:

1. 軟體開發與修改，不論自行開發或委外開發，過程均依照軟體專案架構保留文件及執行內容
2. 委外廠商維護一律使用 VPN 軟體進行加密連接
3. 委外廠商使用之帳號須填寫需求單並在固定期間啟用

六. 資訊資產安全管理

作業:

資訊資產目錄、資訊安全等級、資料輸出管理

執行狀態:

1. 軟體清冊保留完整紀錄，硬體資產清冊每年定期盤點
2. 定義各資訊檔案之安全等級，並執行分類適切性評估作業
3. 資訊安全流程紀錄所有輸出資料規範與內容

七. 業務永續運作計畫之規劃與管理

作業:

緊急應變措施、永續運作計畫

執行狀態:

1. 建立緊急應變還原計畫
2. 每年執行災難復原演練確認緊急應變措施
3. 異地備援

本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)，並納入內部控制作業，除不定期進行資訊安全檢查內、外部稽核，並由稽核室每年將資通安全檢查列入年度稽核計畫之稽核項目，並向董事會報告資訊安全之風險管理執行情形。