資訊安全及個人資料風險管理

業於 115 年 11 月 6 日 第 15 屆第 11 次董事會報告

資訊處

2026/11

Executive Summary（一）：今年做到了什麼

一頁看懂：資訊安全與個資保護的成果

關鍵指標

0 項

高風險問題

年度風險檢查，沒有任何高風險

3 項

重要系統演練完成

主機、虛擬主機與 SAP 都演練過

全年無休

資安監控

24 小時監看，有狀況立刻處理

2 張

國際認證

12 月接受資安與個資兩張認證審查

重點結論

01 制度建好了

資安與個資的規章制度都已訂好；全體同仁定期做詐騙郵件演練與教育訓練；12 月接受兩張國際認證審查。

02 風險控制住了

年度檢查沒有高風險；重要帳號與電腦設備都已清點；備份資料定期測試，確認救得回來。

03 出事救得回來

24 小時監控，有問題馬上處理；重要資料在不同地點各存一份，就算遇到勒索病毒也能還原。

Executive Summary（二）：接下來要做什麼

認證時程與後續工作重點

佳格食品集團

認證時程

2026.10
公司內部自我檢查

2026.11
主管審查會議

2026.12
兩張國際認證
正式審查

2027 起
每年定期複查
持續改善

接下來重點

資安防護升級

- 請專家協助監控系統
- 汰換老舊設備、攔截可疑檔案
- 總部主機備援，壞一台不停擺

個資保護落地

- 自動找出個資放在哪裡
- 防止個資被寄出或外流
- 自動留下紀錄，方便查核

日常管理不鬆懈

- 定期做詐騙郵件演練
- 每年稽核與主管審查
- 發現問題追到改好

報告總覽：ISMS 與 PIMS 推動進程

已執行成果與預計執行項目一覽（①～⑤ 對應後續各頁）

面向	已執行	預計執行
① ISMS 管理面	全員社交工程演練、通識與專責培訓、案例宣導與入侵案例剖析（4 項）	2026.10 內部稽核 → 2026.11 管理審查 → 2026.12 ISO 27001 驗證
② ISMS 實作面	高風險 0 項；3 大關鍵業務演練完成；資產、組態與帳號全面盤點	持續監控，暫無新增項目
③ ISMS 技術面	SOC 整合 7×24 即時應變；異地雙重備份與防勒索還原（Veeam）	機器分析專家服務監控、EOL 汰換與沙箱防禦、總部 HA 雙機備援
④ PIMS 管理面	四階文件制定、高風險個資流向處置、管理審查與改善跟催	2026.12 ISO 27701 初次驗證，其後進入監督審查週期
⑤ PIMS 技術面	規劃與導入準備中	個資自動盤點與分類、全管道外洩阻斷、稽核舉證自動化

① ISMS 管理面：治理推動與驗證進程

對應總覽第①項

已執行

2026 Q2

社交工程案例常態宣導

定期彙整最新詐騙手法與威脅趨勢，深化同仁自主通報觀念。

2026 Q3

社交工程實戰演練

執行全員釣魚郵件防護測驗，強化辨識偽冒郵件警覺性。

2026 Q3

ISMS 通識與專責培訓

完成同仁通識課程與管理專責人員深造研習。

2026 Q3

資安入侵案例剖析

研析外部遭駭案例，檢視集團內部防禦缺口。

預計執行

2026.10

年度內部資安稽核

2026.11

資安管理審查會議

2026.12

ISO 27001 初次驗證

其後進入監督審查週期：2028.10 → 2029.11（規劃）

② ISMS 實作面：關鍵防護執行成效

對應總覽第②項

已執行

風險評鑑結算

0 項高風險

風險值 ≥64 分列高風險，本年度無超標項目。

營運持續演練

3 大關鍵業務

實體主機、虛擬機與 SAP 系統演練完成。

備份媒體管理

全面列管

落實媒體清冊追蹤，完成備份測試與還原查核。

另完成：核心帳號清冊盤點（SAP / DB / OS / 網路 / 門禁環控）、資產與組態精準盤點。

預計執行

既有防護成效持續監控，暫無新增規劃項目。

③ ISMS 技術面：全時監控與災難復原

對應總覽第③項

已執行

SOC 整合 7×24 即時應變

整合網路與資安監控中心，建立即時通報與告警處置程序，強化偵測與應變能力。

異地雙重備份與防勒索還原

關鍵資料跨實體異地雙軌儲存，佈建防篡改備份，縮短復原時間（RTO）。

預計執行

機器分析專家服務監控

減輕 IT 人力負擔，全面可視設備、網路與應用狀態。

EOL 汰換與沙箱防禦

消除 EOL 漏洞風險，強化未知威脅主動防禦。

總部 HA 雙機備援

消除單點故障，確保核心業務不中斷。

④ PIMS 管理面：個資治理與驗證進程

對應總覽第④項

已執行

01

程序文件系統制定

完備 PIMS 四階規範架構，修訂個資保護程序與表單。

02

風險處理與精準抑制

鎖定高風險個資流向進行處置，降低外洩風險。

03

管理審查與持續追蹤

彙整稽核發現事項，研擬並跟催改善計畫。

預計執行

2026.12

ISO 27701 初次驗證

2027.12

第一次監督審查

2028.12

第二次監督審查

取得證書後，各項管控措施持續落實，符合標準合規要求。

⑤ PIMS 技術面：個資即時防護技術落地

對應總覽第⑤項

已執行

目前聚焦技術方案規劃與導入準備。

預計執行

01

自動化盤點與精準分類

自動辨識並標籤化個資，達成敏感資料全面清查與分級。

02

全管道外洩阻斷

管控端點、網路與雲端傳輸，防止機敏檔案不當傳送。

03

落實 PDCA 稽核與合規舉證

自動生成數據流向分析與違規告警，作為驗證技術證據。

Thank you.

活出人生美好的　每一刻！