

資訊安全管理及執行情形

本公司已於115年3月5日第十三屆第七次董事會報告「資訊安全之執行情形」。旭東資訊安全管理及執行情形如下：

(一) 管理架構

本公司由總經理督導資訊部統籌規劃與執行資訊安全政策。於112年8月11日經董事會決議通過，設置「資安專責單位」及「資安專責主管」，並成立資安小組，負責推動資訊安全管理系統（ISMS）相關制度、計畫與活動。

資安組織及分工如下：

1. 資安長：由資訊副課長兼任，負責資安策略規劃與整體督導。
2. 資安管理代表：由資訊室主管擔任ISO 27001管理代表。
3. 資安小組：下設文管小組及稽核小組，由各單位代表組成，負責制度推動、文件管理及內部稽核作業。

資安小組定期將ISMS推動績效向資安長報告，並視需要邀請外部資安專家或顧問參與相關會議，以提升資安治理效能。

內部控制方面，由稽核室依內部控制制度每年執行資訊安全查核；另會計師事務所依據資訊作業環境及財務報表查核需求，辦理資訊環境風險評估及控制測試，以評估資訊作業內部控制之有效性，並定期向董事會報告資訊安全執行情形。

(二) 資訊安全政策

本公司已訂定資訊安全政策並對外揭露，其內容如下：

1. 建置紮實資安制度
2. 建立廠商合作安全規範
3. 養成團隊資安能力
4. 遵守資訊安全相關法規

並以確保系統持續運作、防範外部攻擊、避免資料外洩及強化實體與人員安全為核心目標。

(三) 具體管理方案及投入資通安全管理之資源

為落實資訊安全政策並強化整體防護能力，本公司推動以下管理措施並持續投入相關資源：

1. 資安防護與風險管理機制：
定期執行弱點掃描與滲透測試，並進行修補改善；建立資安事件應變機制，依事件等級執行通報、應變及復原作業。
2. 系統與網路安全管理：
導入防火牆、防毒軟體、郵件過濾機制，並強化端點偵測與回應（EDR）及應用程式白名單等防護措施，提升整體網路與系統安全。

3. 資料保護與備援機制：

建立資料存取控制與密碼管理制度，並執行本地及異地備份；訂定「系統備援及回復計畫」，並定期辦理災難復原演練及ERP資料還原測試，以確保營運持續。

4. 實體安全管理：

實施門禁刷卡管制，並建置機房及重要設備監控系統，以確保關鍵設施安全。

5. 制度導入與驗證：

導入ISO 27001資訊安全管理系統，並設置風險管理機制，定期辦理內部稽核及相關查核作業。

6. 外部專業資源運用：

與國際資安廠商合作進行資安檢測與評估，並視需要邀請資安顧問提供專業建議。

7. 教育訓練與宣導：

定期辦理全員資安教育訓練及社交工程演練（如釣魚郵件測試），並發布資安公告，以提升員工資安意識。

8. 資安人力配置：

設置資安專責人力共計7人（含資安長、管理代表及資安小組成員），負責推動各項資安管理工作。

9. 執行成果：

本公司近年未發生重大資安事件，亦無客戶資料外洩之情形。

(四) 資通安全管理系統驗證情形

本公司已於2026年導入ISO/IEC 27001資訊安全管理系統，並預計2026年7月取得ISO/IEC 27001:2013第三方驗證，後續將持續辦理改版與換證作業，以確保證書有效性延續。

透過該系統之導入，持續強化資通安全風險管理與事件應變能力，確保公司及客戶資訊資產之安全。

(五) 重大資通安全事件

因資訊安全管理的落實，截至2026年4月底未發生重大資安事件。