資通安全管理

(一)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。

1. 資通安全風險管理架構

資訊部內設有資安小組，配置資訊安全專責主管及人員，統籌資訊安全政策制定、執行、風險管理及遵循查核。資訊安全最高主管每年定期向總經理報告資安管理成效與重點議題。

113 年資訊安全執行情形

持續運作資訊安全管理制度，執行資安防護措施並優化制度面與技術面作為，資安專責主管與專責人員配合年度規劃執行各項管理任務。

2. 資通安全政策

本公司資安政策為:「維護公司資通安全，推動資安政策並落實執行，提升整體資安意識。」

資安小組依 PDCA 管理循環機制（Plan-Do-Check-Action）推動資安作業，定期召開會議檢視資安策略與措施適用性。

Plan：參考相關資安制度，訂定資安政策與管理辦法。

Do：多層次資安防護與管理(實體安全、網路安全、權限管理)。

Check：資安持續強化檢查相關制度。

Action：資安措施檢討與改善、資訊安全教育訓練與宣導。

3. 具體管理方案

具體管理方案（114 年度執行）

一.持續強化網路防火牆與網路服務控管，降低攻擊風險。

二.各類電腦設備安裝適用之端點防毒軟體，定期更新病毒碼。

三.作業系統與應用程式定期套用弱點修補更新。

四.核心系統執行年度災害還原演練 3 次。

五.辦理資安宣導與社交工程演練，培養員工資安意識。

4. 投入資通安全管理之資源

民國 114 年企業資訊安全措施推動執行成果：

(1) 完成主機備份系統強化與例行備援測試作業 3 次。

(2) 資訊安全宣導 2 次

(6) 影響營運重大資安事件 0 次。

持續中華電信 HiNet SOC 情資通報服務，接收並處理資安警訊。

強化各廠區資訊系統之資安機制，建立跨廠備援能力。

(二)最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施。

1. 重大資通安全事件：民國 114 年無重大資通安全事件發生。

2. 資通安全風險與因應措施：

面對日益嚴峻的資安威脅(AI 快速生成腳本)(如勒索病毒、惡意程式、系統攻擊等)，本公司持續採取以下措施以提升防禦能力：

評估威脅偵測與應變服務導入(EDR/MDR)。

定期進行弱點掃描與修補管理。

持續擴充資安專責人力並規劃資安證照培訓。

加強資訊安全制度及應變機制，以確保營運不中斷與資訊可用性。