浪凡網路科技股份有限公司

資通安全管理之資訊揭露

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

本公司資訊安全管理與個資管理的最高層級組織是「資通安全暨個資保護委員會」,成員共計 8 位,由資通安全長擔任召集人,下轄「資通安全暨個資小組」、「內部稽核小組」,並由執行秘書監督、管理各小組之日常實務運作。

(二)資通安全政策

為確保本集團所屬之資訊資產的機密性、完整性及可用性，以符合 ISO27001 之要求,使其免於遭受內、外部蓄意或意外之威脅，並遵循 ISO27701 及落實個人資料之保護及管理，符合「個人資料保護法」之要求。

(三)具體管理方案

「資通安全暨個資保護委員會」定期實施管理審查，確保本公司資訊安全與個資保護相關作業的落實。每年延請公正第三方組織依據國際標準之要求實施驗證稽核。前述稽核所發現之不符合事項與改善建議，均須依據本公司「矯正及預防管理程序書」完成改善及存證。

本公司實施之資訊安全管理措施，包含如下：

1、 定期盤點資訊資產及個人資料清冊，依資訊安全及個人資料風險評鑑進行風險管理，)落實各項管控措施。
2、 新進人員皆須簽定資通安全保密協定。
3、 為提升同仁之資訊安全及個人資料保護安全意識與專業知識，每年皆有規劃相關資安教育訓練課程，或派人員接受外單位辦理之專業資安課程，並必須完成一定時數之資通安全訓練，以降低人為錯誤或誤用資通之風險。113 年度資通安全暨個資小組之主管及一般同仁訓練時數為 1 小時，而資訊人員(MIS)為 3 小時，並留存執行成效等紀錄備查。
4、 委外廠商須簽定保密協議，以確保使用本公司的提供資訊服務或執行相關資訊業務者，有責任及義務保護其所取得或使用本公司之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露
5、 重要資訊系統或設備已建置適當的備份、備援或監控機制並定期演練，以維持其可用性。
6、 個人電腦均安裝防毒軟體且定期確認病毒碼之更新，並禁止使用未經授權的軟體。
7、 要求同仁帳號、密碼與權限應善盡保管與使用責任並定期換

置密碼。

8、 已制定資訊安全事件的回應及通報標準程序，由資通安全暨個資小組負責資訊安全事件處置，以適當對資訊安全事件做即時處理，避免損害擴大。

9、 建立業務持續運作管理機制，並定期測試演練，維持其適用性。

10、113 年分別針對資訊安全及個資保護管理各實施 1 次內部稽核，以確保資訊安全、個資保護管理制度之有效性。

11、113 年召開一次管理審查會議，進行全面的管理審查，確保資訊安全與個資保護相關作業的落實。

(四)資通安全管理資源

本公司已通過 ISO 27001：2022 資訊安全管理系統及 ISO 27701：2019 隱私資訊管理系統之第三方驗證，並導入 ISO 27017 雲端服務資訊安全控制措施。其中，ISO 27001：2022 證書有效期限至 2028 年 10 月 30 日，並持續維持相關證書之有效性。本公司亦持續投入預算於資訊安全維運及管理，以強化整體資訊安全防護能力。