遊戲橘子數位科技股份有限公司
2018 年度資訊安全風險揭露

企業資訊安全風險除外部網路攻擊外，內部資安意識及認知不足、病毒威脅等導致系統運作異常或中斷、資料竄改及毀損等後果，均為影響營運主要風險因子。因此針對資安防護作為，公司除明定資訊安全政策作為最高指導，除依循建立相關資安管理組織、規範與作業程序外，並由領導階層每半年定期召開資安會議，檢討公司現有資安作為及擬定改進方案。以下謹就針對公司營運所可能遭遇風險，提出說明及因應作為。

一、員工資安意識不足

由於內部員工所處理的資料、資訊及系統，與公司營運有直接的關係，因此稍一不慎即可能因下載或感染到惡意程式，而影響到公司內部資訊安全。因此公司除將自行編製的線上資安教育訓練，列為必修課程，同時每日蒐集網路上與資安相關報導，不定期針對目前較高風險的資安攻擊手法及安全防護，發佈內部資安公告與實施演練提供相關訊息，加強員工資安意識。

二、病毒威脅

電腦病毒來源可能是所瀏覽的網站、含惡意程式的 e-mail 或、移動式儲存媒體、惡意程式下載...等，因此公司建立多層次的防禦及檢測，終端全面安裝國際知名防毒系統，採中控方式進行監控及防護，以降低遭惡意程式感染及攻擊的風險。

三、網路攻擊

Internet 駭客攻擊將對企業營運是最直接的影響，因此除建置必要防護措施包括重要網段切割與存取授權管制、防火牆、入侵偵測及阻斷攻擊的機制，亦會針對對外提供聯線服務的網站定期/不定期進行弱點檢測與滲透測試、應用程式保護及透過資安弱點通報機制與修補工作，務期將漏洞與被攻擊機率降至最低。另對於惡意的網路攻擊，將彙整相關侵害行為與影響，依法究責。

四、營運中斷

公司針對重要營運服務及資料，均有作必要的同地/異地備份及還原演練，如遇無法避免主營運系統或資料庫毀損或運行中斷時，可於不同服務所律定時效內恢復營運。

五、個資保護

公司於數年前即對早期所蒐集會員個資進行清除作業，並要求各營運單位對於相關資料蒐集應以營運最小化為原則，遵守個人資料保護法，落實各環節處理及保護措施。透過機敏資料遮罩、欄位/資料庫加密及存取授權與告警機制，確保資料安全，並取得 ISO 及 PCI 認證，以稽合程序驗證各處理節點的合理性及嚴謹性。

2018 年度內除發現有遭分散式阻斷服務攻擊及內部少數設備中毒跡象，均及時完成適當因應措施與處置(例:網段阻擋、封包清洗；病毒檢測、掃毒及系統重灌.等作為)，年度內並無影響公司營運重大資安事件。