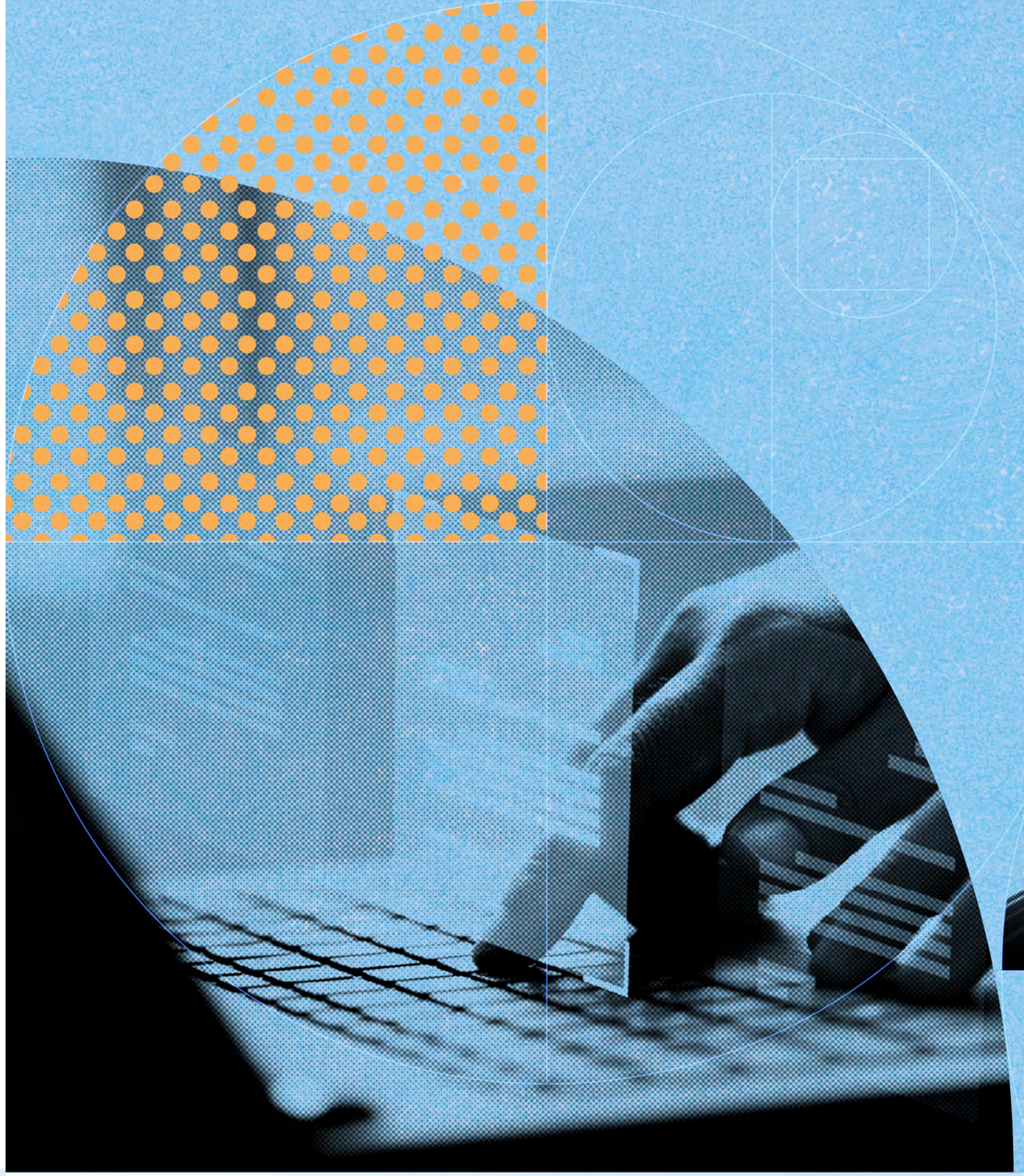


# CHAPTER 02
# 轉動數位責任

gamania
橘子集團



# 2.1 創新投入與專利

## 2.1.1 創新投入與研發

### 創新發展成果

#### 研發策略

橘子持續以消費者需求與市場趨勢爲營運決策核心，透過集團內部各事業群之策略協同與資源整合，系統性推動創新營運管理。在研發策略方面，橘子以建構可長期發展之 IP 與內容生態爲主軸，投入自有 IP 的深化經營及跨平台、跨領域的泛娛樂內容布局，以打造符合新世代消費者需求及文化的社群平台。在產品與技術布局方面，橘子除持續投入行動遊戲與行動生活應用程式之研發外，亦因應數位服務規模擴大與資安治理需求，逐步擴展至雲端應用與資訊安全技術領域。因應人工智慧技術的快速發展，橘子近年亦加速 AI 技術之導入與應用，其中所推出之 B2B AI 商務解決方案「Vyin AI」，以可控 AI 中樞強化非結構化資料處理能力，並透過流程與知識機制降低 AI 幻覺風險，目前已逐步落地於多項實際應用情境。展望未來，橘子將持續評估並擴展 AI 技術之應用深度，朝向建構全生態娛樂網路企業之長期目標推進。

#### 創新研發支出

| 研發支出 | 研發費用占營業收入% | 研發支出年增長率 |
|---|---|---|
| 9.91億元 | 11% | 21.15% |

#### 投入領域

| | | |
|---|---|---|
| AI 應用 | | ● 以智慧中樞作爲系統底層，提供穩定且可控幻覺風險的文字與語音互動服務，並與策略夥伴共同開發長者陪伴機器人，整合自然語意理解、主動風險偵測與擬真人聲技術，穩健拓展 AI 於居家及高齡照護場域之應用。<br>● 結合大規模資料處理與情境理解能力，提供最適切的商品或服務推薦，協助企業建立可衡量、可優化的營運數據閉環。<br>● 投入聲音複製、風格遷移與虛擬人等技術。透過高度擬真的聲紋與圖像生成，將 AI 的應用範圍延伸至行銷科技與實體場域，打造具溫度的數位互動體驗。 |
| 創新 IP 發展 | | ● 持續深化 IP 跨域改編布局，涵蓋小說、音樂、漫畫與影視等多元形式，並以原創內容爲核心，推動 IP 價值延伸。<br>● 透過新星計畫與創作者工作坊培育創作能量，扶植多元新銳作品並導入 AI 應用課程，強化創作者專業能力，並讓同一個 IP 核心更有效率地延伸至遊戲、動畫、漫畫、小說等多元載體，強化 IP 的長期價值與商業潛力，爲 IP 長期發展累積創意與人才動能。 |
| 創新多角化經營 | 遊戲發展 | ● 將 AI 工具與工作流程全面導入遊戲開發的各個環節，實現眞正意義上的「AI-Native 開發模式」。使前期的企劃發想、世界觀建構、角色設計與劇情撰寫，到中期的美術生成、程式輔助、場景搭建與關卡設計，再到後期的品質測試、多語在地化與上線後的營運優化，都能透過 AI 輔助開發，提升整體製作效能與產品競爭力。<br>● 針對不同遊戲類型與功能需求，開發並整合了多種創新 AI 應用，讓 AI 從幕後的輔助工具，進一步走到台前、成爲遊戲內容與體驗的核心組成。<br>● 將 AI 能力深度整合至 Unity 遊戲引擎層級，讓開發團隊能以更直覺、更高效的方式在引擎內直接呼叫 AI 能力。 |
| | 技術研發 | ● 針對《天堂 M》進行玩家行爲分析，透過即時交叉比對與數據整合機制，協助營運團隊更即時掌握玩家行爲與關鍵決策訊號。<br>● 自主研發高性能即時通訊（Instant Messaging，IM）技術，讓集團內部事業單位與外部企業客戶可快速導入通訊服務與管理後台，推動核心技術以平台化方式實現規模應用。<br>● 透過建立集團層級的技術共享制度與導入統一開發工具，強化整體開發一致性，並落實資安風險管理與控管要求。 |
| | 創新投資 | ● 投資「踢帕娛樂」製作的《原子少年 2》，賦能原創 IP 價值鏈的核心實力，從遊戲領航者邁向泛娛樂生態領導者的轉型里程碑。 |

gamania
橘子集團



# 2.1.2 專利與智慧財產權

## 專利策略目標

### 專利策略

遊戲橘子持續追求研發創新，依據營運目標投入必要之研發資源，並建立智慧財產管理計畫，以系統化方式推動相關資產之識別、保護與運用，減少因侵權或不合規而產生的風險。藉由完善智慧財產權管理，有助於降低潛在營運風險與管理成本，提升研發效益與企業整體競爭力，進而鞏固公司在產業中的地位。

### 專利目標

本公司每年定期將智慧財產管理計畫提報至董事會，最近一次提報日期為 2025 年 11 月 6 日。於智慧財產權管理方面，公司在 2025 年設定兩項重點目標 ▶

#### 強化員工智慧財產保護意識

| 2025 年成果 | 2026 年目標 |
| --- | --- |
| 開立兩堂課程：<br>● 專利概念<br>● TIPS 制度<br>共計 146 位同仁完成兩堂課程，課程總時數為 1 小時。 | 持續規劃並實施教育訓練，來深化員工的智慧財產權觀念與知識，以期藉此對內有效保護集團內部智慧財產權；對外降低侵權之風險。 |

#### 精進智慧財產權管理制度

| 2025 年成果 | 2026 年目標 |
| --- | --- |
| ● 自 2024 年開始逐步進行 TIPS 台灣智慧財產管理制度導入之籌備，並於 2025 年正式導入該制度，且於 2025 年 Q4 取得 TIPS A 級認證，證書有效期間為 2025 年 12 月 31 日至 2026 年 12 月 31 日。為當年度同業中唯一取得認證之公司。<br>● 智權規章制度彙整於單一平台，便於同仁取得、參照及獲得相關教育訓練資源。<br>● 同時透過進行權限控管及文件機敏標示，避免公司重要機密外流。 | 持續完善公司智慧財產權管理制度、促進內部智慧財產權管理制度升級，維持 TIPS 認證之成果。 |

gamania
橘子集團



# 智慧財產權基本政策

在數位娛樂快速演進的趨勢下，專利已成爲遊戲產業中保護創新成果與維持市場競爭力的關鍵資產。尤其在遊戲產業中，除了系統架構外，遊戲創新玩法、介面設計等，皆屬於高度依賴創意與技術的智慧財產權，亟需透過專利制度加以保護，以防範抄襲與侵權。爲妥善運用及保護本公司之智慧財產，公司訂有《智慧財產權基本政策》，規劃智慧財產權策略，以降低經營風險、提高企業獲利及取得產業領導地位，並有效避免因侵權而發生的法律風險與經濟損失。自 2025 年起，橘子將關鍵的專利相關制度，優先轉型升級爲符合 TIPS A 級驗證標準之「TIPS 智慧財產管理手冊」，以更高的標準來維護公司智慧財產權。

**策略**

**政策**

| | | |
|---|---|---|
| 降低經營成本與風險 | 智慧財產法律資源運用辦法 | 訊息互通、資源共用，降低法律成本 |
| | 智慧財產保護辦法 | 保護智財不受侵害並避免侵害他人，有效管控風險的發生及減輕損害 |
| | 自製產品商標管理辦法 | 釐清商標權利歸屬，避免集團內重複登記商標之浪費 |
| | 代理產品商標管理辦法 | 得知將代理遊戲時，即進入商標管理流程，以避免商標於各授權地區遭惡意搶先註冊，而徒增營運困擾 |
| | 智慧財產稽核辦法 | 透過稽核方式，監督、落實各智財辦法之執行，以確保策略目標達成 |
| 提高企業獲利 | 專利管理辦法 | 管理集團專利權內容，爲集團累積能獲利的智慧（無形）財產 |
| | 著作權管理辦法 | 管理集團創作內容，爲集團累積智慧（無形）財產 |
| | 智慧財產運用辦法 | 將集團累積之智慧財產，以各種方式大量地運用，以提高獲利 |
| 取得產業領導地位 | 智慧財產獎勵辦法 | 利用獎勵辦法提高集團研發、創作的能力及素質，累積、增加競爭的籌碼，以逐步取得產業領導的地位 |
| | 專利管理辦法 | 有效管理集團內專利研發的能力及資源，拉高競爭門檻 |

註：智慧財產運用辦法、智慧財產保護辦法、專利管理辦法及智慧財產獎勵辦法的專利相關規範，均已整合納入「TIPS 智慧財產管理手冊」中。

gamania
橘子集團



# 2.1.3專利成就

## 創新專利申請

### 專利研發策略

橘子持續強化智慧財產佈局，將專利作爲產品競爭力與研發成果的具體體現。公司之專利研發策略以產品線發展爲主軸，進行關鍵技術的專利申請，確保創新能量轉化爲橘子長期競爭優勢。近年來，橘子專注於 AI 互動技術、大數據分析、沉浸式社群體驗等領域的研發，緊密連結未來與科技趨勢，爲遊戲以外的新興平台應用奠定技術基礎。

### 專利研發運用成果

目前橘子之專利數量在遊戲產業中不僅優於同業平均水平，近三年平均成長率達到 3.05%，接近國際大廠之 3.57%，顯示橘子在技術創新上的穩定累積。透過持續的專利佈局，公司逐步強化自有技術的保護力，以塑造關鍵領域的護城河。

## 歷年專利數統計

橘子深知專利對於企業長期發展與品牌價值的戰略意義，積極投入技術研發與創新成果保護。隨世代趨勢，自 2022 年起更投入於 AI、大數據與社群相關技術，在 2022~2025 年間申請的 47 件專利中，屬於前揭技術的專利共 19 件，其中並已核准 14 件。未來，公司將持續強化研發投入與技術創新，積極取得國內專利權，進一步提升整體市場競爭力。

### 專利數統計

| 年份 | 專利數 | 累計集團專利總數 |
|---|---|---|
| 2022 | 29 | 165 |
| 2023 | 0 | 165 |
| 2024 | 8 | 173 |
| 2025 | 10 | 183 |

gamania
橘子集團



# 2.2 創新成就

## 2.2.1 AI 應用

面對 AI 浪潮驅動全球數位變革，橘子集團於策略轉型的過程中，洞察企業在導入 AI 上的關鍵挑戰，因此 2024 年成立「AI 創新實驗室」，積極佈局前沿技術並擴展國際市場。透過推出企業級創新 AI 品牌「Vyin AI」，致力於提供具可靠性的解決方案，打造具永續競爭力的數位未來。Vyin AI 於 2025 年正式從技術研發期邁入「商業落地與社會實踐」階段。針對企業導入生成式 AI 時普遍面臨的「不可控推理」與「幻覺風險」，Vyin AI 確立了「可控 × 即時 × 效益」的核心戰略。

Vyin AI 以自主研發的「五大中樞架構」爲智慧大腦底層，並結合產業結構化知識，從根本確保 AI 服務的輸出結果具備高度的可預期性與可驗證性，爲企業與消費者提供安全、穩定且負責任的 AI 解決方案。橘子集團將持續秉持「數位責任」與「安全可控」的核心精神，穩健拓展 AI 技術在更多產業場域的應用。


## Vyin AI 核心技術與應用服務

Vyin AI 解決方案提供企業可靈活導入的 AI 服務。我們將自主研發的技術轉化爲具體的商務與社會解決方案，主力推動以下三大應用面向：

**智慧客服與語音對話**
Chatbot & Voicebot

以智慧中樞爲底層，提供高穩定性且幻覺可控的文字與語音互動。2025 年已成功協助知名飯店導入涵蓋五種語系的自動化文字諮詢，並配備智慧化管理後台，讓客戶能自主進行報表分析與內容優化，大幅提升營運決策效率；同時，與策略合作夥伴聯手打造長者陪伴機器人，整合自然語意理解、主動風險偵測及高度擬真人聲技術，將 AI 服務穩健擴展至居家與高齡照護場域。

**精準推薦服務**
Recommendation

結合大規模資料處理與情境理解能力，系統能在多輪的雙向互動中即時解析使用者需求，提供最適切的商品或服務推薦，協助企業建立可衡量、可優化的營運數據閉環。

**虛擬生成技術**
Generative AI & Virtual Human

涵蓋聲音複製、風格遷移與虛擬人等技術。透過高度擬真的聲紋與圖像生成，將 AI 的應用範圍延伸至行銷科技與實體場域，在確保品牌安全的前提下，爲大衆創造具溫度的數位互動體驗。

2025 上半年 Vyin AI 完成多產業與多場景之 AI 應用探索與技術驗證後，下半年起逐步收斂發展方向，聚焦於「語音互動」及「機器人 AI 大腦」兩大核心領域。透過整合語意理解、即時推理、語音處理與系統串接能力，持續強化 AI 於眞實互動場景中的可控性、即時性與整合性，並進一步推動相關技術於客服、零售、智慧照護與機器人應用等場域之落地發展，作爲未來產品化與規模化拓展之核心基礎。

# AI 應用場景

在上述 AI 核心技術與組合應用基礎上，橘子進一步將相關能力落實於具體營運與服務場景，推動 AI 自實驗性應用邁向可規模化之商業落地。透過聚焦實體互動與決策支援等關鍵，Vyin AI 持續驗證技術於實務運作中的效益，深化智慧服務、機器人應用與跨場域整合之發展。

## 文字客服機器人

橘子導入集團自研之 AI 客服 Vyin Chatbot，建構以 AI 爲核心之智能服務協作模式，重塑客服營運架構。透過「AI 優先處理、人工承接例外」之分級服務機制，有效提升服務效率與一致性，並優化人力配置，推動客服營運由人力密集型態，逐步轉型爲具備規模化能力的智慧服務模式。

在實際服務運作上，AI 主要承接高頻、標準化之客戶問題，提供即時且一致之回應；眞人客服則聚焦於複雜查核、客訴處理與例外情境判斷，進一步強化整體服務品質與應變能力。爲確保服務穩定性與風險控管，Vyin AI 運用「幻覺可控、風險可控、流程可控」的技術核心，透過產業結構化知識確保回覆的安全與零風險，並支援第三方 API 串接以實現與既有系統的無痛整合。同時，於眞人服務流程中導入 AI 文本輔助生成工具與信心判斷機制，作爲回覆品質控管依據，降低人爲判斷差異，提升整體回應正確性與服務一致性，並強化服務流程之標準化與可追溯性。

目前 AI 已可處理近 50% 之標準化問題類型，有效降低重複性案件量，並將簡單案件平均回覆時效由約 8 分鐘縮短至 2 分鐘內。2025 年全年累計約 13 萬筆自動應答對話，自主解決率達 97%（年增 1%），顯示 AI 於標準化問題處理之成熟度持續提升；全渠道約 47%（年增 12%）服務需求可於 2 分鐘內完成處理，有效分散高峰期服務壓力並提升整體服務韌性。同時，人力資源逐步轉向高價值服務內容，提升複雜問題處理能力，進一步強化整體服務效能與客戶體驗。透過 AI 客服與眞人協作機制，本公司持續優化服務即時性與一致性，平均首次回應時間縮短 71%（24 小時降至 7 小時），全年即時客服滿意度穩定維持在 94% 以上。AI 客服不僅提升服務效率，亦有效降低等待時間與溝通落差，進一步強化客戶對品牌之信任與黏著度。

除集團內部運用，Vyin AI 文字客服機器人也已成功於知名飯店導入涵蓋五種語系的自動化文字客服機器人，該系統不僅能處理即時的旅客諮詢，更配備了 Chatbot 智慧化管理後台。透過此後台，客戶端能夠自主進行報表分析與內容優化（持續自主學習優化），大幅提升了營運端的決策效率與資訊更新的即時性。

1
全年累計約 13 萬筆自動應答對話，自主解決率達 97%（年增 1%）

2
全渠道約 47%（年增 12%）服務需求可於 2 分鐘內完成處理

3
平均首次回應時間縮短 71%（24 小時降至 7 小時），全年即時客服滿意度穩定維持在 94% 以上

## 機器人軟體升級

面對生成式 AI 的浪潮，多數企業嘗試導入 AI，但多數專案仍停留在概念驗證（Proof of Concept，PoC）階段，難以轉化爲實質的營運價值。深入觀察實體機器人市場後，橘子發現兩大應用斷層：一是缺乏「人味」的互動（難以打斷、缺乏上下文理解），二是互動僅停留在被動問答，無法有效引導商業決策或服務體驗。因此，Vyin AI 致力於結合「智慧對話中樞」與「精準推薦系統」，將 AI 從單一的對話工具，升級爲能創造雙向互動與商業閉環的決策大腦。

在開發過程中，團隊面臨的最大挑戰在於大型語言模型（Large Language Model，LLM） 如同「黑盒子」般不可控的推理機制，容易產生幻覺與品牌風險。此外，傳統 AI 語音處理檢索增強生成（Retrieval-Augmented Generation，RAG）流程動輒需要 5 至 8 秒，疊加推薦系統後甚至超過 13 秒，嚴重影響使用者體驗。爲解決此痛點，團隊以自主研發的「五大中樞架構」搭配結構化產業知識，從根本確保輸出的可預期性與品牌安全；並透過大小模型靈活協作與全鏈路工程優化，成功克服了速度與理解力難以兼顧的瓶頸。

gamania
橘子集團



Vyin Ai 機器人的核心架構建立在「可控」與「即時」兩大基礎上。相較於市面現有技術，橘子達成了三項具代表性的突破，成功打造極低延遲的即時體驗：

1. 將語音回應延遲大幅縮短至 2.5 秒內，實現接近眞人的反應速度。

2. 非線性的對話彈性：具備多輪語意理解能力，支援使用者中途插話或自由切換話題，打破傳統機器人制式的線性對話框架。

3. 即時精準推薦：支援千萬商品 / 知識規模等級的即時檢索，能在 0.5 秒內完成情境解析與推薦，將互動轉化爲可衡量成效的數據資產。

# 桔利 AI 居家陪伴機器人

隨著台灣於 2025 年邁入超高齡社會，長照人力吃緊與照護品質不均問題日益嚴峻，橘子回應高齡照護需求，積極將 AI 技術應用於智慧照護領域，與策略合作夥伴女媧創造聯手推出「桔利 Gilee」長者陪伴機器人。這項源自 MIT 的創新解決方案，融合 Vyin AI 的可控智慧大腦與女媧創造的人形互動設計，讓陪伴不只停留在對話，而是升級爲守護長者情緒、健康與安全的貼心夥伴。該應用不僅整合了 Vyin AI 的自然語意理解與主動風險偵測技術，並具備由新竹台大醫院提供保健知識問答功能。此外，透過高擬眞的 AI 仿聲技術，能生成家屬聲音爲長者讀信，以無幻覺的陪伴對話與情緒偵測機制，爲高齡社會提供具溫度的科技解方。

## 桔利應用場景

當長者表示「胸口悶、會喘」，桔利能立刻關切、提供專業健康建議並同步通知家屬。

若遇疑似詐騙，則會提出警示並建議撥打 165 專線或聯繫子女，達到即時雙向守護。

## 桔利體驗回饋

中化銀髮總經理李宗勇及團隊回饋：「桔利外型討喜，尤其是仿聲語音信功能，能讓長輩聽到家人的聲音、感受到關懷，這是很重要的設計。」

## 2025 年成果

於「台北國際照顧博覽會」首度公開亮相，並開放現場互動體驗。

gamania
橘子集團



## 文化創作與營運支援

除發展 Vyin AI 解決方案應用外，橘子亦積極探索 AI 技術在文化創作領域之可能性，導入 ACGN（動畫、漫畫、遊戲、小說）領域，不僅提升創作者創作效率，亦能改變用戶體驗，實現更加個性化和多樣化的創作方式。我們計畫針對以下幾個面向結合 AI Agent 概念，助力 ACGN 領域的創新發展。

### 劇情創作 Agent

針對劇情創作，不僅輔助創作者快速構建故事，還能指導劇情發展、角色互動與對話設計。可實現 AI 自動優化內容，提供風格調整、情節分支與文化適應，並支持多媒體創作，有助於高效創作獨特故事。

### 漫畫設計 Agent

針對漫畫設計，可自動生成分鏡圖、場景設計與角色互動，根據劇情要求提供畫面構圖建議，並幫助創作者快速完成草圖、背景設計和細節繪製。同時也能協助調整角色姿勢、表情以及畫面風格，讓漫畫創作過程更加流暢和高效。

### 遊戲互動 Agent

針對遊戲開發，可提供智能化的遊戲關卡設計、角色互動和挑戰系統生成，根據玩家的行爲和反饋優化遊戲內容，提升遊戲的互動性和沉浸感。並整合 AI NPC、AI BOSS、任務與關卡生成及測試代理等創新應用，將 AI 由開發輔助角色推進爲遊戲內容與體驗核心。

同時，橘子也利用 AI 進一步擴大在營運中的應用：

### 遊戲測試 Agent

可進行自動化遊戲測試，包括功能測試、性能測試和除錯，快速發現並報告錯誤，檢查功能是否符合設計要求，實現調整測試過程，減少人工測試時間與成本，確保遊戲品質、流暢性和穩定性。

### 專案管理 Agent

可實現即時監控專案進度，根據任務完成情況生成進度報告，並及時向 PM 發出風險預警。如果發現專案進度滯後、資源不足或存在其他潛在問題，AI 會提出調整建議，協助 PM 提前應對風險。同時，AI 可自動執行大量的管理任務，減少公司對人工的依賴，從而節省人力成本，團隊可以將更多的精力投入到創新和核心業務之中。

gamania
橘子集團



# 2.2.2 創新 IP 發展

2025 年，橘子持續推動 IP 跨域應用與商業化發展，串聯漫畫、小說、遊戲、影視、品牌聯名等不同領域，建立更具彈性的內容應用與合作模式，將原創故事延伸至影視改編、音樂跨界、周邊商品等多元場景，擴大 IP 內容於年輕世代與數位娛樂市場的影響力。在國際布局方面，亦積極拓展授權合作，成功將原創漫畫輸出至海外市場，提升創意內容的國際能見度與商業價值。透過健全跨界生態圈，橘子持續爲台灣創意人才搭建商業化舞台，支持文化內容永續發展，驅動台灣原創動能走向國際。

## 兩大 IP 孵育計畫

| 計畫名稱 | 計畫內容 |
| --- | --- |
| 挺音樂！音樂靠山計畫 | 邀請台北流行音樂中心合作，透過宣傳資源、演出機會、獎金等各式支持方式，爲音樂人建構完整的資源網路，並運用 AI 技術協助音樂人行銷宣傳及粉絲經營。 |
| 文創股長 | 跨足圖文產業，搭建圖文 IP 孵育計畫「文創股長」，目前已有百位創作者進駐。從課程培訓、品牌媒合、宣傳曝光等不同方式，實際提供創作者資源，同時爲各 IP 做圖像授權洽談。 |

## 原創三大計畫

| 計畫面向 | 2025 年成果 |
| --- | --- |
| 跨域改編 | ● 原創 BL 小說《HowHow 夢遊腐境》 ● 音樂專案《看你聽的》第三彈 ● 影視改編漫畫《第一次遇見花香的那刻：花開之後》 ● 遊戲前傳漫畫《九日—李耳傳》 |
| 新星計畫 | ● 創作者平台共選出 21 部新星作品推廣 |
| 人才培育 | ● 創作者工作坊共兩場：<br>■ 線上課程 - 曾建華老師「你的創作夥伴：AI 漫畫助手升級啦！」<br>■ 實體課程 - 朱宥勳「AI 時代．小說創作工作指南」 |

gamania
橘子集團




# 《結緣金》
## 實境互動節目

全台首檔由 AI 虛擬偶像主持的實境節目《結緣金》已於 2025 年 11 月 1 日正式開播，並同步於 YouTube「宮祈緣」與「霹靂台灣台」官方頻道播出。節目由橘子集團 AI 虛擬偶像「宮廟少女—宮祈緣」（暱稱小緣）擔綱主持，以「一日職人體驗」爲核心主軸，帶領觀衆探索漫畫、命理、都市傳說與音樂等多元領域。

該節目由橘子與霹靂國際共同製作，採取「橘子主技術、霹靂主內容與文化」的分工模式，橘子集團的原創中心主導技術與虛擬角色開發、G Studio 虛擬攝影棚、行動互動裝置等虛實整合技術；由霹靂擔任《結緣金》的節目製作方，負責節目製作與敍事與文化監修，目標是打造「科技＋文化」的新型態節目。霹靂方面更將此合作視爲「台灣原創精神在數位時代的延續」，希望透過 AI 虛擬偶像拓展傳統文化與數位娛樂的結合形式，示範「用科技放大而非取代傳統文化」的實踐路徑。

《結緣金》以文化 IP 的導流與擴散機制爲核心亮點，以線上節目串連 MOJOIN《肥羊重生後》條漫與霹靂旗下的素還眞、談無慾連動，搭配小緣傲嬌、嗆辣又可愛性格的「媽祖乾女兒」形象設定，拉近與觀衆的情感距離，實踐跨域的 IP 結合擴散。同時結合 Wirforce 等線下參與轉化爲節目內容，讓虛擬偶像不再只是螢幕角色，而是能介入眞實文化活動，形成線上節目、社群內容與現場活動的串聯。

gamania
橘子集團



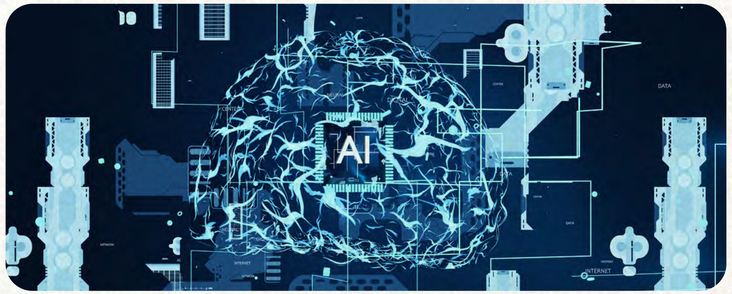
# 2.2.3 創新多角化經營

## 多角化的橘子

### 多角化經營願景與策略

長期以來，外界對橘子的認知多以遊戲產業爲主，然而集團近年來積極推動業務多元化轉型，整合代理、自研及科技應用三大發展軸線，強化整體競爭優勢。在代理業務方面，透過大數據分析深化與原廠之合作關係，並結合在地行銷與社群擴散能力，提升產品經營效能，凸顯橘子作爲代理商的策略價值；在自研領域，將多年遊戲營運經驗導入產品規劃，並憑藉累積之海外行銷與市場經驗，持續拓展遊戲營運版圖。同時，橘子亦積極掌握科技趨勢，導入 AI Agent 與大數據技術，提升作業效率與產能，打造更具彈性與深度的在地服務價值，支撐長期多元成長與永續經營。

橘子集團以「內部研發孵化」與「外部策略擴張」雙軌並行的經營策略，推動數位創新與產業價值升級。在內部，我們鼓勵技術創新並提供創業資源，將研發成果轉化爲具商業競爭力的產品；在外部，透過策略性獲取國際雲端平台（如 AWS、GCP）認證，我們加速關鍵技術產品化，並將服務範圍由台灣本土延伸至東南亞等國際市場，厚植集團中長期的技術韌性與產業領先地位。




### 多角化經營成果

| 聚焦領域 | 2025 年成果 |
| --- | --- |
| 遊戲營運 | • 推出第二款跨平台 MMORPG 遊戲《救世者之樹 M》，持續擴張台港澳玩家群體。<br>• 《新楓之谷》於 12 月推出睽違 2 年半新職業改版，創下 12 月扣點歷史新高。<br>• 承襲先前自研專案的經驗，全新自製肉鴿遊戲（Rougelike）類型手遊開發。 |
| 技術研發 | • 根據動態標籤專利，完成天堂 M 營運後台開發與建置，透過將每日標籤邏輯擴展至玩家行爲，交叉比對下使營運更能即時掌握玩家關鍵動向。<br>• 自主研發高性能即時通訊（Instant Messaging，IM）軟體開發工具套件（Software Development Kit，SDK），具備支撐高併發需求的穩定性，將集團核心技術轉化爲具備國際競爭力的軟體即服務（Software as a Service，SaaS）底層通訊支柱。<br>• 透過標準化 SaaS 服務模式，提供集團各事業單位及外部企業客戶快速導入與應用 IM 通訊技術與管理後台，實現技術資源的規模化應用。在無需撰寫程式碼的情境下，用戶能直接透過管理介面輕鬆調整客製化需求，降低合作夥伴的技術門檻並提升營運效益。<br>• 透過建立集團技術共享機制與導入統一開發工具，落實資安風險控管規範。 |
| AI 應用 | • 運用過往詐騙樣態大數據，結合 AI 自動化預警技術，事先監控潛在高風險帳號，準確度可達 60% 以上涵蓋率。<br>• 透過 AI 進行每日客服數據解讀，摘要重點與擷取關鍵議題，協助營運日常掌握整體狀況並及早發現潛在風險。透過分析數據趨勢，協助判斷問題影響程度與支援決策，並可同步檢視全產品數據，有效評估各服務間的影響，從被動應對轉爲主動管理。<br>• 發展 AI 幕僚，涵蓋用戶動態數據、外部情報兩類服務，協助營運人員整合內外部數據，綜合判斷每日遊戲生態內與市場變化。搭配 AI 對話式查詢，進行深入剖析取得洞察，提升營運掌握度。<br>• 透過 AI Agent 將散落在不同平台（交易網站、遊戲論壇、社群、影音平台等）的用戶及競品正負面聲量進行交叉分析，即時掌握產品動態，協助判斷產品策略方向。<br>• 將傳統的單向指令模式升級爲雙向對話互動系統，透過擬人化與個性化的遊戲體驗，提升數位內容的沉浸感，強化用戶的黏著度與留存率。 |

gamania
橘子集團



# 創新投資

橘子透過多角化投資，轉動數位創新責任，致力於在擔任資金投入者的同時，更扮演著數位資源與生活價值的聚合者。透過策略布局前瞻技術新創、在地文創 IP 與美學生活虛實整合品牌，成功將服務邊界從虛擬娛樂延伸至用戶的實體生活場景。此外，我們也協助新創團隊、創作者與品牌接軌市場，並結合 AI 與大數據分析共同探索前瞻領域，縮短創新商業化週期。此布局不僅強化集團在「泛娛樂數位生活圈」的競爭優勢，更具體實踐帶動產業升級、促進多元人才永續發展的社會責任。


2025 年，由橘子集團策略投資之「踢帕娛樂」製作的《原子少年 2》，憑藉卓越製作規格與創新偶像培育模式，榮獲第 60 屆金鐘獎「綜藝節目獎」。此項指標性榮譽，不僅肯定了集團在影視內容的深度布局，更象徵橘子已成功跨越單一遊戲產業框架，展現其賦能原創 IP 價值鏈的核心實力，達成從遊戲領航者邁向泛娛樂生態領導者的轉型里程碑。

透過踢帕娛樂的創新經營，集團成功串連數位內容、社群互動與實體商機，不僅爲台灣娛樂產業注入新血，更展現經營指標性原創文化 IP 的深厚底蘊。展望未來，橘子集團將持續深化娛樂產業的策略布局：

**技術加持**
透過數位平台與 AI 技術賦能，擴展多元化的藝人與節目合作。

**人才培育**
扶植新世代創作者與偶像團體，打造具高度互動性與永續性的內容生態。

**產業共榮**
持續推動跨域整合，落實數位內容產業共存共榮的長遠願景。

gamania
橘子集團



# 2.3 資訊安全

## 2.3.1 資安管理

### 資訊安全政策

本公司訂有由執行長核定之《集團資通安全政策》，作爲本集團建立資訊安全與網路安全管理制度、程序及電腦系統軟硬體等相關資通管理之準則，旨在確保公司重要資訊之機密性、完整性及可用性，同時遵循「上市上櫃公司資通安全管控指引」，藉由 ISO 27001 標準之規範，不斷校修集團資通安全政策。該政策之主要內容包括：定期執行資訊安全管理系統之評估與檢討、持續接收內外部威脅情資並進行風險評估及測試、要求全體員工遵循相關規範並即時通報資安事件；同時，針對第三方合作夥伴進行安全評估，於合約中納入資訊保護相關條款。

除對內的安全防護，橘子持續關注供應鏈安全議題，對於資訊作業安全執行之供應商管理，公司在原有的資訊作業委外基礎之下，增加重要或關鍵供應商安全要求；對於委外作業涉及跨境個資傳輸，需依據集團「個人資料檔案安全維護計畫」及「個人資料檔案系統設備暨軌跡安全維護計畫」辦理。

在網路安全管理構面，明定建置環境時應使用必要之防護措施，包括：防火牆區隔、網段切割、安全通道存取設計規劃、使用加密通訊協定、設有入侵偵測及阻斷攻擊等機制。針對對外提供服務之網站定期或不定期進行相關之安全檢測（如：資安健檢、弱點掃描、滲透測試等）並修補弱點。集團將核心系統或服務納入資通安全威脅偵測管理（Security Operation Center，SOC），24 小時持續不間斷觀察實時情況，於必要時主動攔阻外部侵害，同時導入使用外部資安評級工具，用以瞭解曝露在外之風險，進行弱點修補。

### 資訊安全組織架構

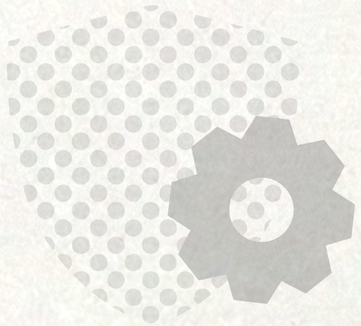
「集團資通安全管理委員會」（以下簡稱資安委員會）爲本公司資通安全的最高指導組織，由集團董事長暨執行長擔任最高督導，董事長自公司成立以來具備豐富資安治理經驗，同時擔任集團旗下資安公司雲力橘子法人代表，負責全面監督與檢視各項資訊安全管理措施的落實，充分展現集團對資通安全制度的高度重視與支持。委員會成員由各部門指派專員組成，成員層級涵蓋首長與處級主管等職，並設置「資安主管」一職，由資訊服務處之處級單位統籌管理資通安全相關事務，另委請專業資安技術團隊協助提供各項資安服務。2025 年委員會召開兩次會議，由集團執行長主持，針對資安管理制度的執行情況、營運風險評估、資安專案進度及因應對策進行整體檢討與決策，確保資安策略與營運需求保持一致。在集團營運策略及政府法令法規指導下，委員會負責制訂整體資安政策，推動資安防護措施部署、系統漏洞補強、異常事件掌握及重大事件應變。

橘子全面導入 PDCA（Plan—規劃評估、Do—設計建置、Check—覆核稽查、Act—檢討改善）管理循環，確保風險管理制度「說寫做一致」，並以持續改善爲核心，提升營運與服務的安全韌性。透過風險評估、政策滾動修訂、防護建置、監控管理與弱點補強的完整循環架構，持續追蹤最新資安趨勢，靈活調整因應不同的資訊服務模式、營運環境與法規要求，確保資訊系統與網路服務能在可控風險範圍內穩定運作。

為強化資通安全治理與執行效能，集團於資安委員會下設立多元職能小組，包括政策暨資安技術推行小組、執行小組、查核小組、風險小組及應變小組。《集團資通安全組織管理辦法》明訂各小組權責，以持續推動資通安全相關事宜，回饋資安治理之安全管理指標。各小組分工合作、相輔相成，詳細工作分配如右圖所示。

同時，資訊單位亦定期進行資安評量、資訊資產盤點、營運系統清查、界定營運衝擊（包括 MTPD、RTO、RPO）以及資安量測。

我們持續關注組織適用之法規修訂情況，即時校準集團資通安全相關管理制度。資安委員會每年定期召開資通安全管理審查會議，審查資通安全制度管理與落實之執行成效、研議強化資通安全管理方向，商議或提供資通安全管理制度執行所需之相關資源，確保集團資安治理符合法規與監管要求，以降低資安風險、強化防護，因應不斷變化的資安威脅。



gamania
橘子集團



# 資訊安全管理策略與措施

## 資訊安全管理策略

本公司資安策略關注人員、制度及管理三大面向，遵循國家法令，通過風險導向的分析與管控，管理客戶及會員數據資產。

### 人員

分群實施教育訓練，提供一般同仁資通安全通識課程訓練，針對資訊人員開展功能性資安講座或課程。

### 制度

遵循上市上櫃資通安全管控指引，同時借鑑 ISO 27001 標準，校修或新增資訊作業管理相關規範。

### 管理

透過明定資安委員會各小組職責，定期會議、宣導資通安全政策及相關安控要求，即時檢討實作情況與反饋。

橘子持續朝「全生態科技企業」之目標，積極落實「永續轉動」的核心策略，引入外部資安風險與安全管理績效評級，評級優良可以提升企業品牌形象，吸引潛在客戶或合作夥伴，進而提高企業整體價值，同時讓投資人了解公司資安管理的表現、資安體質的健康程度，進而成爲投資決策的重要參考依據。

## 資訊安全管理措施

| 管理階段 | 管理方式 |
| --- | --- |
| 事前預防 | **定期檢討資訊安全相關管理規範**<br>● 每年依照現行法令法規、產業脈動、利害關係人之要求，進行資安政策及相關管理規範、程序編修作業，內容涵蓋資料保護、營運安全、資訊作業委外、密碼管理等共計 13 項規範。<br><br>**資訊作業安全檢測**<br>● 依據不同的資訊作業服務性質及風險進行營運業務資安分級、設定必要防護作為，並定期進行各項資安管理評量；對於資通服務系統進行安全檢測、辦理網站或主機弱點掃描、滲透測試，要求系統上線前或重大變更時，依據風險等級評估結果，執行相應之安全檢測，並完成系統弱點修補，降低人為或自然因素對企業營運所造成的衝擊；同時也藉此了解、評估企業網路環境及系統安全狀況，驗證目前資安防護設定的安全等級與成效。<br><br>**導入資安監控（SOC）與端點偵測及應變機制（Endpoint Detection and Response，EDR）**<br>● 偕請國內第三方資安技術顧問團隊監控並掌握資安告警及威脅情資，強化並加速偵防與回應。<br><br>**資通安全作為有效性檢討**<br>● 集團資安委員會每年定期召開兩次會議，針對資安策略與機制進行滾動式的檢討與修正，同時檢討規範落地執行之成效並追蹤內部查核發現。<br><br>**導入 ISO 27001 等國際資訊安全管理標準**<br>● 集團各分子公司取得國際資安認證（具體情形請參閱資安認證一覽表）。<br>● 橘子支付自 2019 年起連年取得「行動應用 App 基本資安檢測」認證，並經第三方檢測機構通過。<br><br>**培養員工資安意識**<br>● 透過模擬駭客攻擊手法、打造仿真度極高的攻擊模擬郵件，寄送誘騙信件給員工，藉以了解員工資安意識的真實狀況與面對社交工程、網路釣魚等行為的基礎防衛能力；對於誘騙成功的員工施以針對性的教育，喚起員工面對此類威脅的本能反應，引以調整資安應對行為、建立資安防護停、看、聽的反應力。2025 年對全員工進行電子郵件社交工程，累計發送 3,978 封釣魚郵件，驗證同仁對於釣魚信件的偵察能力。<br><br>● 由資安風險驅動教育訓練，讓主動防禦位於攻擊之前，透過內部適當的資訊安全講習，提升資通管理人員及一般同仁資安認知及意識、了解資訊安全重要性及各種可能的安全風險、提高員工資訊安全意識、進而改變行為。2025 年集團全員必修課程之完訓率及合格率達 100%。<br><br>● 透過資訊服務協作平台「資通安全專區」，每週整理資安新聞與時事，提供與工作或日常相關的實用安全指南短文，以及不定期派送資訊安全電子報輔以資安意識宣導，藉此提升及鞏固企業員工對於資安意識警覺性、培養安全檢查的習慣。<br><br>資安新聞與時事：388 則　資安實用安全指南：11 份　資安電子報：3 期 |

| 管理階段 | 管理方式 |
| --- | --- |
| 事中執行與檢核 | **營運資訊作業自我評量**<br>● 針對各項資安管理措施設定評量機制，定期要求各營運分子公司進行資訊作業自我評量。<br><br>**端點安全管理**<br>● 設有端點防護機制，有效降低端點設備因不慎使用而形成的資安缺口。<br><br>**重要系統、資料庫及檔案皆具備份機制**<br>● 集團已建立完整的營運持續與災難復原計畫，涵蓋關鍵系統、資料庫與檔案之備份機制，並定期（每年至少一次）執行災復演練。演練內容包含書面模擬與實際情境測試，以確保還原 IT 基礎架構存取權和功能的有效性，確認在發生異常時能即時恢復存取權限與系統功能，快速恢復至企業正常或可接受的營運水準，以達到核心服務系統持續運作、企業營運不中斷。<br><br>**年度資安內部查核作業**<br>● 每年由集團總部擬定實施資安管理檢核計畫，對各營運分子公司進行訪談與抽樣各項資訊作業執行情況，並將查核結果提報集團資安委員會，查核發現則列管追蹤矯正情況，作為精進集團資安管理依據。2025 年度訪查後的精進規劃包含：次年度階段性擴大資安查核的範圍、規劃資訊作業委外相應的安全管理措施，以及逐步推動全組織員工對於資訊資產的知識，規劃發展各分子公司輕量化之風險評鑑方法論。 |
| 事後應變與復原 | ● 建立資安應變及通報機制，確保資安事件可迅速及完善的處理與復原，同時增設資安事件回顧管理機制。<br><br>● 2025 年未發生重大的網路攻擊或事件，亦未曾涉入任何相關之法律案件或監管調查。 |

註：EDR 即端點偵測及應變機制，是結合即時持續監控、端點資料蒐集以及進階交叉關聯，用於偵測並回應主機和端點連線的可疑活動，可讓資安團隊更快速地判斷及交叉比對分析，並提供更明確的偵測事件。

## 資安技術提升

為因應快速變化的數位威脅環境，遊戲橘子持續強化資訊安全技術，透過政策制定、人才培育、即時監控及產業交流等多面向措施，提升資安防護韌性。在技術部署上，依各子公司營運特性與風險樣態導入客製化防護措施，針對不同設備、業務需求及資料敏感度，制定量身訂製的資安策略，確保各公司都具備最符合實際需求的資安防護能力；同時推動制度化資安人才培育，透過證照補助與專業訓練，強化紅藍隊、數位鑑識等能力，並促進跨部門參與，2025 年資安證照數較去年成長逾 20%，顯示培育成效顯著；此外，橘子也持續精進資安監控中心，導入即時安全監控儀表盤，並擴大集團監控範圍，隨時掌握系統及網路資安狀態。同時結合 AI 賦能，透過指令總結搜尋結果、智能摘要資訊與關聯訊息，降低人工反覆檢查、分析所需的時間。

### 資安管理專業性

截至 2025 年底，本公司同仁在資安管理方面的累計持證張數共 44 張。

| 資安證照發證機構名稱 | 2025 年底持證張數 |
|---|---|
| Amazon Web Services（AWS） | 13 |
| CERIAS[註] | 1 |
| EC-Council（國際電子商務顧問局） | 13 |
| Google Cloud Platform | 14 |
| ISC²（International Information System Security Certification Consortium，國際資訊系統安全認證協會） | 1 |
| PMI （Project Management Institute，美國專案管理學會） | 2 |

註：此證照多由台灣在地法人機構（如中華民國電腦技能基金會 CSF、中華資訊安全專業人員協會）與美方或科技大廠技術合作發證。

### 資安教育訓練

橘子支持員工參與資訊安全相關課程，通過外聘顧問進行專題講座、開展內外部訓練等方式，加強員工在資訊安全方面的認知及技術能力。此外，橘子也在 2025 年針對種子窗口辦理個資安全維護計畫教育訓練課程，計畫 2026 年將本課程列為全員必修，以提升同仁個資保護之安全意識。

| 參與對象 | 課程名稱 | 參與人數（人） | 總時數（小時） | 完訓率（%） |
|---|---|---|---|---|
| 全體員工 | 駭客如何針對企業進行網路攻擊 | 1,208 | 305 | 100% |
| 資訊人員 | 安全軟體開發生命週期 | 37 | 37 | 100% |
| | 資安威脅趨勢與案例分析 | 37 | 74 | 100% |
| | 資料保護 | 37 | 55.5 | 100% |
| 特定人員 | 電子郵件社交工程教育訓練 | 121 | 121 | 100% |
| | 個資安全維護計畫教育訓練 | 43 | 86 | 100% |

## 供應商資安管理

橘子在原有的資訊作業委外開發安全基礎上，增加供應商安全管理要求（含複委託之範圍與責任），對於第三方開發、建置、維護、處理與管理之活動，須依照其功能可能涉及之資安風險嚴重程度，具備相對應之資安檢測項目（包括重要數據隱私要求）以及評估對承案之核心成員，另行簽訂保密協議；合約須將委外安全規定納入合約（包含委外之資訊系統或環境出現異常與發生資訊安全事件時，需依組織之「資安事件通報及應變作業」進行相關程序之處理），同時也須約定服務終止之資料保留及刪除要求、保留對供應商稽核之權利，確保每個供應商承諾應用足夠的技術和組織措施保護其處理的資訊。

資安檢測廠商資格需具備資安專業證照或是使用之檢測工具須同於國際檢測工具之標準，促使各分子公司委外開發系統於導入或上線前具備一致之安全基準。「集團營運事業資安管理要點」亦設有系統或服務正式上線前之各項安全檢測要求。

此外，橘子於 2025 年底檢修「個人資料保護政策」及「個人資料檔案安全維護計畫」等，提升組織團隊在處理、進行組織數據交換時（包括個資、跨境傳輸等）的保護要求，確保所有供應商協議均包括適當的陳述和保護的義務；同時規劃進行供應商抽樣查核，實際確認委外供應商的資訊環境水準。

gamania
橘子集團



# 資安風險管理

橘子積極落實「集團營運事業資安管理要點」，持續強化營運資訊系統各項重要元素的安全強度（如：網路、作業系統、資料庫、應用程式等），提升資訊安全管理制度的完整性，確保資訊系統穩定運作，保護資訊設備與資料文件安全，避免遭受各類威脅侵入與破壞，進而降低營運作業風險。除了完善的管理措施外，亦須持續監測潛在風險，並確保於風險事件發生時具備即時應變與有效處置能力。因此，針對任何可能對營運資訊作業構成威脅的因素，橘子進行安全指標資料之蒐集，並要求相關資訊系統與服務實施定期或不定期之安全檢測，藉此提升防護效能、維持營運服務水準、保障客戶權益。

## 資安風險管理目標

資安風險管理爲持續性的循環機制，透過管理機制進行資通安全營運風險分析及影響評估，建立適當防護機制、監控措施及應變作爲，從而使公司營運做到最小化損失和最大化收益。集團資通安全目標如下：

1. 維持集團之資通系統持續運作
2. 防止駭客、病毒等外部威脅惡意入侵及破壞
3. 防止人為意圖不當及資訊資產之不法使用
4. 防止機敏資訊外洩
5. 避免人為疏失意外
6. 維護實體環境安全

## 辨識之資安風險與因應措施

| 資安風險項目 | 可能影響 | 因應措施 |
| --- | --- | --- |
| 律法及標準合規性 | 2025 年 11 月 11 日經政府公告「台灣個人資料保護法」修法，賦予個人資料保護委員會（個資會）統一的主管機關地位與執法權限，重新調整公務機關與私人機構之監督架構，包含明訂個資事故之報知與通報義務、行政檢查、相關罰則。 | • 密切關注修法草案，經公布「台灣個人資料保護法」修正後即進行組織之「個人資料保護政策」、「個人資料檔案安全維護計畫」及「個人資料檔案系統設備暨軌跡安全維護計畫」之檢修，用以落地執行各環節資料處理與保護。 |
| 網路攻擊 | 企業資訊技術人員自身不安全的規則設定或未依規辦理的資訊作業程序，將有機會讓不肖人士使用技術手段或方法，透過管理漏洞，入侵、破壞或是竊取目標系統、網路，直接衝擊企業營運。 | • 透過相關資訊作業管理辦法，明定建置環境時應使用必要之防護措施，包括：防火牆區隔、網段切割、安全通道存取設計規劃、使用加密通訊協定、設有入侵偵測及阻斷攻擊等機制。<br>• 針對對外提供服務之網站定期或不定期進行相關之安全檢測（如：資安健檢、弱點掃描、滲透測試等）並修補弱點。<br>• 將核心系統或服務納入 SOC 資安監控，24 小時持續不間斷觀察實時情況，於必要時主動攔阻外部侵害。<br>• 透過資安情資蒐集之弱點警示，進行系統強化或漏洞修補，以期減低因弱點而遭受攻擊之機率。 |

## 辨識之資安風險與因應措施

| 資安風險項目 | 可能影響 | 因應措施 |
|---|---|---|
| 病毒威脅 | 瀏覽過的網站、電子郵件中含惡意程式的附件或連結、社交媒體網站的惡意連結或執行檔、可攜式儲存媒體、未經驗證文件、檔案、軟體或應用程式、不安全的存取權限設定等皆可能攜帶病毒。 | • 透過硬體升級與雲端技術，建構全域多層式資安防護網，從端點防護的防止內部設備遭入侵，到網路邊界防護的阻擋外部攻擊，形成自動化防禦，另有安全監控中心全天候的資安監控，即時掌握系統或服務安全情況，降低遭惡意程式感染及攻擊的風險。<br>• 每年於不特定期間對企業員工進行電子郵件社交攻擊演練，使用擬真度較高的郵件對企業員工進行測試，用以驗證同仁對於不安全郵件的警惕程度，對於成功誘騙的同仁施以針對性教育訓練，並於課後評測學習成效，同時也分析錯答題型，作爲日後教育訓練課程編撰的調整基礎。 |
| 營運中斷 | 資通系統無法持續運作，將停止對外提供營運服務，影響品牌形象、營收、客戶及股東信任及權利受損。 | • 依據「集團資通安全政策」、「集團營運事業資安管理要點」，每年要求針對營運核心服務進行資訊作業營運持續演練，驗證系統還原後能持續服務、確保機敏資訊之安全性，演練包括事件通報處理，藉由完整的演練讓相關同仁熟悉事件處理步驟，強化資安事件應變能力，減少營運衝擊，降低服務、資產及財務損失風險。 |
| 員工資安意識不足 | 員工因職責所需，直接接觸公司營運系統及資料，未依安控要求操作、非安全的使用習慣或處理方式、甚至是將公司配發的資訊設備不慎遺失且未妥善進行必要之處置，該設備可能會使用到不明軟體、感染惡意程式，因而洩漏營運之機敏資料，影響到公司內部系統安全、營業秘密、資料外洩，引發資安事件。 | • 導入使用資料外洩防護工具，掌握機敏資料「流動樣態」，即時偵測識別、阻擋資料外洩行爲及外傳管道分布；降低員工操作不當之資料洩露機會。<br>• 教育訓練課程分設不同領域（全員、資訊人員、特定人員），適職務屬性辦理分衆化課程，提升員工資訊安全意識；同時鼓勵從事資訊技術職務的同仁，參加各式資訊安全、資訊作業管理之研討會，瞭解新興產業動態、資安趨勢及技術，藉此提升風險預判能力。年度訓練情況詳見 2.3.1 資安管理 - 資安教育訓練。<br>• 不定期透過資訊服務協作平台「資通安全專區」發布資安相關資訊及報導，建立員工資安基礎知識、降低不慎操作而造成資安風險的機會。<br>• 透過社交工程演練驗證員工資安意識，提升員工對隱私權、個資法、數據保護實踐和網路安全行爲等認知。 |
| 供應鏈安全管理 | 第三方廠商資訊環境的規模、運作機制的成熟度，不在可管理監控的管理範圍內，攻擊者可以利用這些薄弱的面向，繞過管理嚴格的企業本身，從企業信任的供應商或協力商進入企業內部，脆弱的供應商十分考驗委外的資料安全保障。 | • 透過「資訊作業委外與供應商安全管理規範」採取合理的資訊安全措施及保護機制要求（如：安全開發、權限管理、多重驗證、資料存取控制、保密協議、跨境傳輸、事件 / 故通報、契約終 / 中止之資料返還與刪除、稽核權利要求等）。 |

gamania
橘子集團



# 資安通報與處理程序

遊戲橘子透過「資安事件通報及應變作業」界定資安事件分類、分級標準（含升、降級）以及通報與處理層級。對於相較過往之變動，統一對資通安全組織之執行小組成員召開說明會，要求將相關異動資訊進行單位橫向宣導，同時於公司電子告示板刊登「資安事件 24 小時通報專線及通報專用信箱」資訊。

## 資安事件通報流程

集團全體同仁皆有舉發事件之責，並須第一時間主動通報所屬單位 IT 技術窗口，窗口將依據事件類型與嚴重程度進行初步釐清，並填寫「資訊安全事件通報紀錄單」，後續由資訊部門聯同相關單位展開後續資安事件處置。資訊單位需在預定的處理時限內完成事件排除與解決，並於處理結束後，提供事件分析報告及改善建議，以預防同類事件再次發生。所有資安事件的處理結果與報告將定時彙整，提供資訊安全委員會議檢視留存。

在資安事件 / 故處理與回應時效上，設有專責人員追蹤處理進度，依照分級標準要求時間追蹤、記錄，隨著處理時間、狀況進展及衝擊程度變化，則依據「資安事件升級與降級標準」決定升級或降級，追蹤的時效與週期亦隨時況調整。

**Step 1** 發生資安事件，立即依流程通報 IT 技術窗口

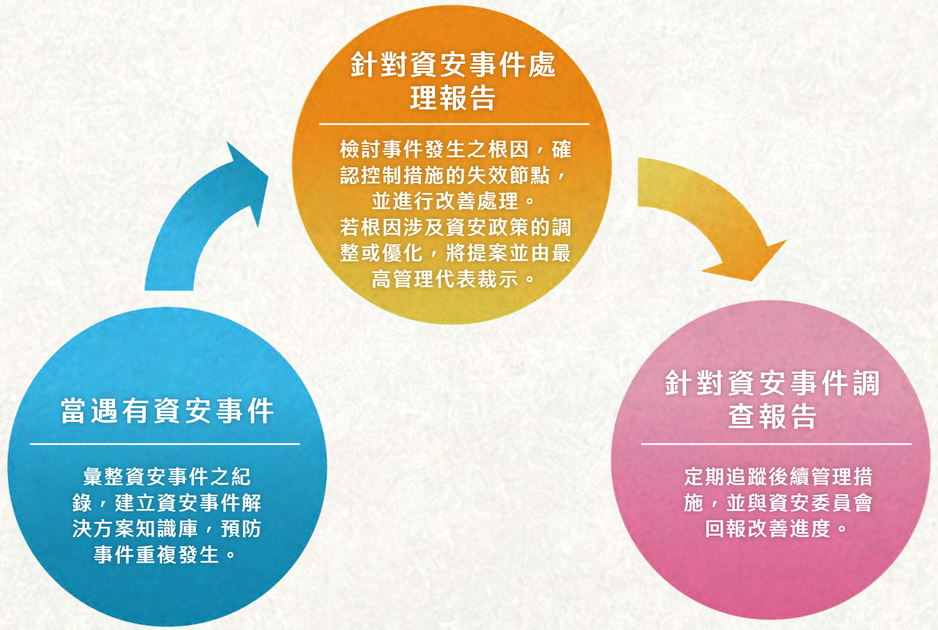
**Step 2** 依事件類型與等級，填寫「資訊安全事件通報紀錄單」

**Step 3** 由資訊單位與相關部門協同排除事件，於目標時限內完成處理

**Step 4** 處理後提出事件分析報告與修補建議，防止同類事件再次發生

## 資安事件處理程序

針對資安事件，公司設有回顧管理之機制，目的在於將事件影響帶來的教訓，作爲未來強化資安防護的重要依據。每當發生資安事件，相關單位將彙整事件之紀錄，與資安委員會應變小組共同檢討事件發生之根因，確認控制措施失效環節並提出改善對策。若事件根因涉及資安政策面的調整或優化，則提報資安委員會最高管理代表裁示。事件處理完成後，公司將建立資安事件之解決方案知識庫，作爲後續教育訓練實務參考，進一步提升公司應變事件之效率與資安防護能力，並定期追蹤改善措施，確保落實成效。截至 2025 年年底，集團未發生資安事故。



gamania
橘子集團



# 引領業界資安重視

雲力橘子積極舉辦資安論壇，旨在構建跨企業交流的平台，促進企業間對資安議題的認知，共享實務經驗。2025 年舉辦之 Hacker Talk 駭客論壇，引導企業資安意識上的「策略調整」與「痛點捕捉」，上半年聚焦由被動防禦轉向主動防禦，強化企業對結合 AI 進行威脅預測之策略認知；下半年進一步以駭客視角解析未來 AI 攻擊趨勢，協助企業將資安由技術議題提升至攸關企業存續之避險意識，成功喚起高階決策者對前瞻布局的重視。

此外，橘子也積極參與外部相關會議，分享資安實務經驗，例如參與亞馬遜雲端運算服務（Amazon Web Servies,，AWS）高峰會與 Google Cloud Summit，協助企業認知人工檢查在規模化環境下所承擔的高度負擔，進而轉向採用自動化資安基準檢查機制（如 Amazon Q 應用）；也在中華民國資訊軟體協會北中南巡迴中，藉由數發部資安署與健保署的權威分享，結合雲力橘子的「資安韌性治理」架構，推動政府機關重新檢視既有的資安防護模式。

2025 年 CYBERSEC 臺灣資安大會中，橘子以「新世代 MSSP 資安威脅聯防」爲主軸，聚焦協助企業因應雲地混合架構下日益複雜的資安風險。分享內容著重於如何突破地端與雲端之間的技術邊界，整合 SOC、威脅偵測與應變服務（Managed Detection and Response，MDR）及雲端原生應用程式保護平台（Cloud-Native Application Protection Platform，CNAPP），建構具整合性與即時性的智慧監控與防禦體系。會議上，橘子進一步說明 MSSP 如何運用即時偵測與自動化回應機制，協助企業快速因應現代化攻擊手法，降低人工作業負擔並提升整體防護效率；同時，針對雲端原生應用的資安議題，提出可兼顧資料安全、法規遵循與軟體開發效率的防護策略，協助企業在數位轉型過程中能兼顧軟體開發速度與資安合規性。

綜合橘子於資安領域之長期耕耘經驗，建議企業可依循政府訂定之資通安全管理法，從策略、管理、技術及認知教育四大面向建構關鍵防禦。其中，在策略層面，企業應建立制度化的資安政策並取得高階管理階層的支持；管理層面則建議導入資通訊安全管理制度標準（如 ISO 27001）並定期辦理內部稽核；在技術層面，落實必要防護與定期安全檢測；同時，透過持續的資安教育訓練，全面提升組織整體的資安意識與防護韌性。


## 資安領航者— 橘子的資安目標

橘子透過長期累積的資安實務經驗，奠定從傳統服務轉向智慧化、自動化資安領航者的實力，更精準鎖定了企業在後轉型時代「核心戰略與自動化防護」的剛性需求。針對 2025 年參加「CYBERSEC 台灣資安大會」，身爲橘子集團的資安管理專家，雲力橘子設定了明確的核心目標。以下是具體的目標設定與達成期待：

- 正式宣示「雲力橘子」新品牌
- 推廣「雲地混合架構下的智慧防線」，聚焦 SOC + MDR + CNAPP 的三合一聯防架構，定義「新世代 MSSP」市場標準。
- 鎖定金融、製造、零售等正處於數位轉型深水區的企業買家，深耕跨產業潛在客戶。
- 利用 Cyber Talent 專區與職涯演講，直接與新世代資安人才對話，搶占資安關鍵人才。

gamania
橘子集團



# 2.3.2 守護網路安全

因應數位時代下產業數位轉型的發展，橘子深知資訊安全與每個客戶息息相關，已是企業穩健營運的重要基石。爲迎戰瞬息萬變之資安挑戰，我們持續強化整體服務的可靠度，致力於提供數位環境之資安三要素—CIA：機密性（Confidentiality）、完整性（Integrity）與可用性（Availability），達成企業及客戶雙贏之永續發展。

在實務上，本公司導入防火牆、入侵偵測系統（Intrusion-detection system，IDS）和入侵防禦系統（Intrusion-prevention system，IPS）等資安系統，並建置全天候資安監控服務 SOC，由資安團隊即時分析網路流量與異常行爲，強化整體風險應對能力。同時，本公司亦成功取得 ISO 27001 資訊安全管理系統認證，定期進行系統漏洞掃描與滲透測試，主動發現並修補潛在安全風險漏洞。我們與業界夥伴密切交流，並透過多種管道取得並分享最新資安情資，確保資安防護機制持續更新，有效防護客戶最重要之資產。

此外，本公司對所提供的產品與服務，皆清楚揭露使用方式與注意事項，確保資訊透明與使用者知情權。透過預先擬定之契約條款與合法標示，保障消費者獲得正確資訊，維護其財產、身心健康與數位權益。透過這些持續性的努力，橘子集團致力於打造一個安全、可靠的網路、雲端環境，保護用戶的資料與隱私，並確保業務順利運作，進而維持營運不輟之重要使命。

## 犯罪防制

隨著網路資訊蓬勃發展，詐騙行爲與盜取遊戲帳號等問題頻頻發生，成爲新型態的社會挑戰。橘子秉持以服務客戶至上、玩家權益優先的態度，積極投入數位犯罪防制行動，與大衆消費者站在同一陣線。對於接獲的相關申訴案件，只要具備充分佐證資料，橘子團隊即主動配合，協助消費者應對犯罪行爲，防堵不法投機者危害平台安全。

自 2022 年起，橘子攜手 165 全民防詐騙網站，設置線上查詢機制，司法警察可透過系統即時提交查詢案件需求，大幅提升查辦效率。同時，考量數位遊戲術語專業度高、辨識不易，集團成立獨立運作的「聯防小組」，派遣專人 24 小時輪班支援，提供警察、檢調單位即時資訊說明與疑問解答服務，確保防詐作業不中斷。

「詐欺犯罪危害防制條例」於 2024 年生效，將網路業者納入本法管制範圍，其中第 36 條 ~ 第 38 條規定與網路連線遊戲業者相關，規定網路業者須協助阻斷詐騙訊息、保留紀錄並配合查詢。對此，法務與營運單位協助配合事項如下，以共同應對不法行爲：

於收到警方或主管機關通知我方服務有疑似涉及詐欺犯罪之情事者，對於涉及詐欺犯罪情事之用戶暫停提供服務。

於收取詐欺相關案件之調取通知三日內提供資料，並依上述法定期限保存資料。

**2025 年成果**

**(1) 持續與政府相關單位合作防詐**

- 7 月：加入信用卡聯防機制，在警政機關或發卡行通報異常交易時，橘子安排鎖定帳號或取消交易，即時降低受害者損失。
- 12 月：加入數發部電商暨高風險網頁聯防機制，透過營運 / 風控等相關單位通報，主動防堵潛在風險網站，杜絕玩家受騙可能性。

**(2) 內部持續觀察詐騙案件樣態，優化風控管理措施**

- 7 月：旺季詐騙捲土重來，透過分析詐騙案件樣態找出破口，故於 8 月 1 日起緊急關閉遭濫用之機制，8 月 13 日推出新防堵機制，案件穩定下降。

**(3) 導入 AI 防詐預警，針對高風險帳號預先監控列管**

- 下半年：運用過往詐騙樣態大數據，結合 AI 自動化預警技術，事先監控潛在高風險帳號，準確度可達 60% 以上涵蓋率。

gamania
橘子集團



# 數位內容責任

遊戲橘子以數位娛樂多媒體內容爲主要產品與服務，致力於提供玩家與消費者創新、優質的數位體驗，所有上架內容均嚴格遵循營運所在地之相關法規規範。在民主社會的開放網路環境中，言論表達更爲自由，可能衍生出不當內容的曝光風險。作爲平台經營者，橘子主張應建立明確的責任內容準則，以展現我們對永續商業理念的重視與實踐。

## 廣告倫理

2023 年啟動「集團廣告倫理政策」，爲國內同業首家針對廣告主訂定廣告業務相關規範，並統合集團泛數位娛樂事業體之回饋，藉以提高本政策之適用性及作爲產業示範。本政策內容除適法外，亦針對成人內容、管制商品、娛樂、健康等產品分類設定管制條件，並禁止一切暴力仇恨、騷擾、欺騙性文字以招攬或誤導消費者，如違反，橘子有權停刊該廣告。例如 2024 年橘子旗下電商事業體購物橘子，全面遵循本政策，針對數位隱私保障之蒐集、高風險內容識別之警語與要求合法素材使用權等，進一步落實行動，確保廣告內容誠實無虞。

在數位廣告與行銷服務過程中，橘子重視廣告內容之眞實性、適切性與社會責任，避免誇大不實、誤導性表述或可能引發爭議之內容，並依循各平台規範與內部審查原則進行把關。針對客戶提供之素材與文案，皆於上架前進行內容檢視與確認，確保不涉及侵權、不實陳述、違反公序良俗或其他不符作業規範之情形，以降低合作與投放風險。同時，服務過程中亦重視個人資料保護與資訊安全管理，針對資料接觸、傳遞與使用等環節依循相關規範審愼處理，降低資料外洩與不當使用之風險。

## 責任內容

本公司所發布的遊戲及平台，於註冊頁面重點聲明使用者應遵守本公司營業規章、管理規則、網際網路國際使用慣例與禮節之相關規定，嚴禁任何違反公序良俗等行爲，禁止上傳或發布包括但不限於：暴力、性暗示、仇恨言論、恐怖或極端主義思想、錯誤資訊、網路騷擾、自我傷害、歧視性等生成式內容，情節重大者本公司有權終止任何數位服務。

同時，橘子重視素材使用之合法性，於專案執行中留意圖片、文字、影音及設計元素之授權與使用範圍，避免侵害第三方智慧財產權，維護合作雙方權益。針對不同數位平台之上架與審核機制，橘子於專案執行中配合平台政策進行內容調整與送審作業，針對敏感視覺元素、文案用語及呈現方式進行修正，確保內容符合規範並順利上線。面對內容審查、客訴、爭議素材或平台退件等情形，橘子也透過跨部門溝通、內容修正與反覆確認機制，強化風險應變能力，將數位內容責任落實於日常營運流程。

## 兒童保護

本公司所產生之數位內容，爲促進兒童青少年重視身心均衡發展，皆鼓勵年滿 12 歲以上的自然人使用，並依照《兒童及少年福利與權益保障法》、《遊戲軟體分級管理辦法》規定，提供合適之數位內容及明確分級標章，採取避免兒少接觸之必要措施，並明確標示相對應之警語。爲尊重兒童及青少年的隱私權，所發布之遊戲及平台，皆於使用者條款中提醒，對於未成年用戶或玩家，要求其法定監護人同意方可蒐集其個人隱私或敏感資訊。同時，若家長 / 法定監護人有發現異狀，聯繫客服後，本公司將採取適當措施保護兒童及青少年隱私。

爲強化全體員工對內容責任之認知，確保營運過程中數位內容之妥善管理，集團相關權責單位統籌辦理涉及數位內容責任相關之教育訓練，集團各單位配合參與。訓練主題涵蓋個人資料保護、著作權與素材使用、內容與廣告法規遵循、品牌安全及危機應變等，以提升同仁在內容製作、媒體執行與客戶服務過程中的責任意識與風險管理能力。

| 課程名稱 | 受訓人數 | 總訓練時數 |
|---|---|---|
| 個資安全維護教育訓練 | 991 人 | 1709.8 小時 |

註：此教育訓練數據包含實體課程及線上課程。

gamania
橘子集團



# 行動裝置資安防護方案

隨著數位轉型加速推進，現在的 App 已並非單純的前端工具，而是直接連到企業核心系統（API/Cloud/Payment）、承載帳號資訊、金流資料及個人資料等高度敏感資訊，因而成爲潛在的攻擊入口。攻擊者可能透過繞過既有安全機制發動攻擊，對企業資訊安全與營運穩定性構成威脅。橘子透過行動裝置資安防護產品 appGuard，能有效解決包含逆向工程、改包攻擊、執行時攻擊、環境風險偵測以及資料保護等問題，爲企業在「App 層」補上資安最後一塊防線。目前 appGuard 已經在金融業、遊戲產業、電商或政府 / 公共服務被採用，其效益廣泛包含防詐騙、防帳號盜用、確保網路交易安全及防止資料外洩。

行動資安正由以規則與程式碼檢測爲主的靜態防護模式，逐步演進爲結合動態監測、人工智慧分析與整體系統架構治理的整合性防護體系。2025 年 appGuard 針對行動裝置資安防護的強化關鍵如下：

- **將執行階段應用程式自我保護（Runtime Protection，RASP）納入標準防護機制：**
  使 appGuard 的防護範圍由程式碼層級延伸至執行階段，透過即時監測應用程式行爲，主動偵測並即時阻擋攻擊行爲，以降低應用程式於實際運行期間遭受入侵之風險。
- **人工智慧驅動攻擊與人工智慧驅動防禦（AI-driven Attack vs. AI-driven Defense）：**
  面對攻擊者日益運用人工智慧技術進行弱點探測與攻擊行爲的趨勢，防禦端亦須導入人工智慧技術，透過行爲分析（Behavioral Analysis）與異常偵測機制。
- **應用程式介面安全（API Security）與應用程式安全（Application Security）之整合性防護：**
  透過整合應用程式、應用程式介面（API）與後端系統（Backend System）之資安控管，建立端到端的一致性防護架構。
- **行動裝置零信任架構（Zero Trust for Mobile）：**
  不預設信任任何裝置或執行環境，並於每一次存取行爲中執行身分與風險驗證。透過持續驗證與最小權限控管機制，降低行動裝置於不可信環境中遭受攻擊或濫用的風險。
- **供應鏈攻擊風險（Supply Chain Attack）：**
  隨著行動應用程式高度依賴第三方軟體開發套件（Third-party Software Development Kit，SDK），相關元件已成爲主要攻擊途徑之一。供應鏈弱點可能在未經察覺的情況下導入惡意程式碼，對整體應用程式與後端系統造成重大資安風險。

未來 appGuard 將進一步升級爲結合資安情資分析與決策支援的智慧化資安平台，實現由防護走向情報與洞察的轉型，其提升策略包含：

- **由攻擊防護邁向資安情報驅動：**
  透過系統性蒐集應用程式於執行階段所偵測之攻擊事件與異常行爲數據，進行關聯分析與模式辨識，並將分析結果回饋至防護策略調整機制，形成持續優化的閉環式資安治理流程。
- **整合人工智慧資安技術（AI Security）：**
  appGuard 將持續導入人工智慧技術於應用程式資安防護中，重點包含行爲分析、攻擊預測及自動化防禦。
- **建立 App、API 與雲端環境的一體化防護架構：**
  未來 appGuard 將發展爲全堆疊行動資安平台（Full Stack Mobile Security Platform），以降低跨層級配置錯誤與資安落差風險。
- **與 SOC 之整合：**
  appGuard 所偵測之應用程式攻擊事件，將可匯入 SOC，並進一步整合至安全資訊與事件管理系統（Security Information and Event Management, SIEM），形成完整防禦體系。

gamania
橘子集團



# 2.4 客戶權益保障

## 2.4.1 服務與溝通

為持續保障消費者與客戶於各類產品與服務中的權益，本公司於 2025 年進一步強化服務治理機制。除持續遵循政府主管機關相關法規與國際準則外，亦導入數據化與標準化之管理架構，確保服務流程具備一致性、可追溯性及可監控性，提升整體服務品質與治理透明度。

在服務模式方面，持續深化 AI 與自動化應用，優化智能服務協作機制，提升回應效率與服務品質穩定度，並強化高峰期間的服務承載能力，以降低等待時間與重複進件情形。同時，依據不同客群需求進行分級服務設計，透過差異化服務機制確保關鍵客戶之服務體驗。

在溝通渠道方面，維持全年無休、24 小時不中斷之服務體系，整合電話專線、官網留言板、即時線上對談及智能 Chatbot 等多元渠道，並持續優化前端引導與問題分流機制，提升問題解決效率與資訊傳遞清晰度。透過跨渠道整合與服務流程優化，致力於打造即時、順暢且具一致性的客戶服務體驗，進一步強化企業與客戶間之信任關係，作為長期營運與永續發展之重要基礎。

## 客戶申訴機制

為持續保障顧客權益並強化服務品質，本公司持續優化客戶申訴處理機制，建立多元且即時之受理管道，確保客戶意見能即時受理與回應。當顧客提出申訴時，第一線客服將即時建單並轉交相關單位進行查核，原則上於 1 個工作日內啟動回應流程，並依案件複雜度於 3 至 5 個工作日內完成處理與回覆，所有案件均完整留存並納入定期品質檢視與持續改善機制。針對較高風險或具爭議之案件，公司設有跨部門協作機制進行複查與決議；若客戶對處理結果仍有疑義，亦可透過主管機關或第三方單位提出申訴，公司將由專責窗口統一對應，並於 15 日內完成回覆，確保處理程序之公正性與合規性。

2025 年整體申訴處理效率維持穩定，公機關申訴案件 15 日內如期結案率持續達 100%。隨著 AI 客服應用深化，透過前端即時回覆、問題引導與資訊透明化，有效降低重複性與誤解型申訴發生，整體申訴量持續呈下降趨勢（年減 14%），顯示服務準確度與前端識別能力進一步提升。透過標準化流程與 AI 輔助機制，本公司持續強化申訴處理效率與品質，降低溝通落差，並提升顧客對服務體驗與品牌之信任，作為落實顧客權益保障與永續經營之重要基礎。

## 專業客服體系

優服橘子作為橘子集團的客服專家，於 2025 年持續推動客服體系升級，除深化 AI 客服與自動化應用外，亦進一步擴展為顧客關係管理（Customer Relationship Management，CRM）合作經銷與導入顧問角色，提供法人客戶更全方位之客服與顧客關係管理解決方案。透過整合 AI 客服、流程自動化（Robot Process Automation，RPA）、AI 輔助文本生成及 CRM 系統導入能力，打造具規模化與彈性調整能力的智能服務體系，推動客服營運由傳統人力委託模式，轉型為「智能服務協作」之數據驅動服務模式。

### 整合 AI 與 CRM 能力，升級法人專案合作模式

- 2025 年除持續優化 AI 客服應用外，進一步結合 CRM 系統導入與流程自動化能力，協助法人客戶從客服營運延伸至顧客關係管理整體規劃。透過整合對話數據、會員資料與服務指標，建立跨系統數據視角，協助客戶即時掌握用戶行為與服務成效。
- 透過導入顧問與專案管理機制，提供系統規劃、成效追蹤與優化建議，使優服橘子由服務執行角色，進一步轉型為協助客戶優化營運與決策之策略合作夥伴。

### 強化數據回饋與治理機制，落實品質閉環與法遵管理

- 在既有多元回饋機制基礎上，2025 年進一步整合 CRM 與客服數據，強化回饋資料之集中管理與分析應用。透過滿意度調查、客服回饋、案件紀錄及品質抽檢結果之整合分析，建立問題歸因與追蹤機制，形成完整的品質改善閉環。
- 客服營運持續依循主管機關規範，落實回應時效、紀錄留存、個資保護及申訴處理流程，並透過定期稽核與制度優化，確保服務品質與合規性穩定提升。

### 推動規模化智能服務，強化體驗一致性與品牌價值

- 2025 年進一步將智能服務協作模式由單點應用擴展至多場景與跨渠道服務，結合 CRM 數據應用與客戶分級管理機制，提升服務精準度與資源配置效率。透過 AI 承接標準化需求、人工處理高複雜情境，建立穩定且一致的服務體驗。
- 透過整合服務數據與客戶洞察，協助法人客戶優化用戶經營策略，提升高價值用戶之互動品質與服務滿意度，進一步強化品牌信任與用戶忠誠度。

gamania
橘子集團



# 2.4.2 個資與隱私保護

橘子在資訊安全管理上採取多層次防護機制，所有網路服務皆建有防火牆、網路身分辨識與威脅監控分析機制，能及時偵測並阻擋惡意網路行為，確保服務穩定與用戶資訊安全。我們亦定期進行系統弱點掃描與修補作業，透過模擬駭客攻擊與資訊安全演練，持續強化應變能力。同時，依據不同服務類型設置相對應的資料備份作業，以降低突發事件所帶來的風險。為確保資料存取安全，僅限經授權之人員得以接觸相關資料，詳細資訊請參閱 2.3 資訊安全。

橘子重視個人資料的保護，訂有明確的《個人資料保護政策》，適用範圍涵蓋集團分子公司之所有員工及其供應商，並由集團層級的「個資管理委員會」負責統籌管理。凡於集團內處理個資之單位（包含全體員工、承包商及合作異業所管理之個資），皆須依規定規劃、執行並落實個資保護相關作業，同時定期向委員會報告推動進度與落實情況。

## 個資保護政策與原則

橘子針對個資蒐集遵循九項原則，於蒐集時即主動告知使用者隱私權保護政策及使用者條款，堅守不蒐集不必要個資之原則，並充分保障用戶選擇權，告知其是否接受行為追蹤、個人化行銷與資料的二次目的使用。

凡涉及網路傳輸之資料均啟用加密機制，以防止資料傳輸過程中遭第三方非法擷取。與消費者或供應商簽訂之合作協議中，皆簽署保密條款，嚴禁未經授權之資料提供、銷售、交換或出租予其他團體、個人、私人機構或其他用途。橘子秉持「零容忍」原則，對資安與個資保護進行處理，凡違反者將依據內部「獎懲辦法」實施必要處置。2025 年並未發生侵犯客戶隱私事件，亦無與用戶隱私有關之法律裁罰。

### 個資保護九項原則

**目的明確化原則**
目的必須在蒐集當時就闡述明確，並重視隱私權政策聲明並且尊重當事人之權益。

**公開與告知原則**
個資資料之開發、運用、政策等必須遵循一致公開規定。

**限制蒐集原則**
明確定義個資類別與其相關之蒐集限制條件。

**限制利用原則**
個資應用需經由當事人同意，處理及利用均需經適當申請取得授權核可。

**個人參加原則**
當事人對其個資進行查詢、閱覽、製給複製本、補充或更正、要求停止蒐集、處理或利用及刪除等權利須予以保障，並在適當時限內回應。

**資料內容原則**
依據當事人自主或蒐集時限屆滿等符合資料使用之目的，並確保資料之正確性、完整性和時效性。

**安全管理原則**
資料必須採取合理、適當之安全保護措施，以防止資料遭遺失、盜用、毀損、竄改或揭露的風險，並符合法定通報要求。

**責任義務原則**
釐清個資資料主管單位、監督人員及使用者，做好權限、職責管理劃分要求。另應將個資保護義務與責任，明確要求集團同仁遵守，避免個資不當運用。

**預防損害原則**
對於個資蒐集、利用及傳輸時，受到威脅損害的可能性與嚴重性，有即時通知與處理機制，降低預防因個資保護不當所造成的賠償與刑罰風險損害。

gamania
橘子集團



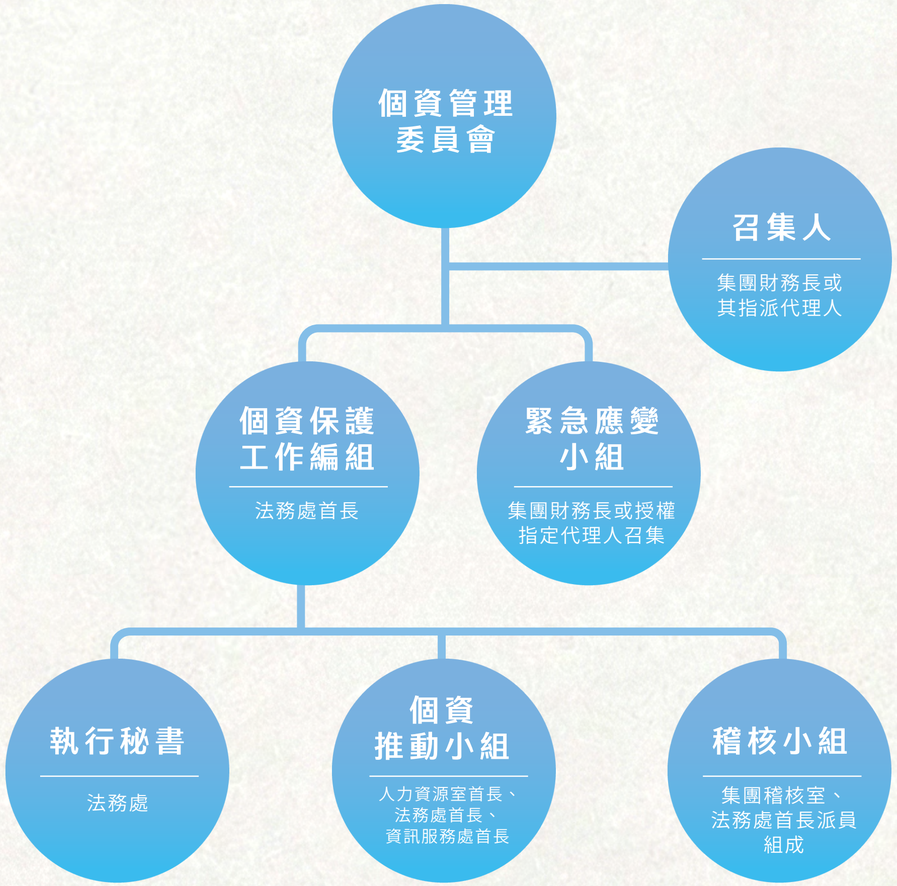
# 個資管理委員會架構與執掌

個資管理委員會由財務長擔任召集人，轄下設有緊急應變小組及個資保護工作小組，並與法務處協作，共同防堵外部入侵風險，確保個資檔案的正確性及完整性。個資保護工作小組納編「稽核小組」，由稽核室與法務處成員組成，負責規劃定期檢核作業與安全維護措施的執行情形，並於第一時間進行改善作業，確保制度有效落地。

## 個資管理委員會之執行任務

1. 個資保護政策之擬議
2. 個資管理制度之規劃及相關事宜討論、推展
3. 個人資料隱私風險之評估與管理審查
4. 集團所屬各級單位專人與員工之個資保護意識提升及教育訓練計畫之擬議
5. 個資管理制度適法性與合宜性之檢視、審議及評估
6. 其它個資保護、管理之規劃及執行事項


## 個資管理委員會組織架構圖



gamania
橘子集團



# 2.4.3 客戶滿意度

## 2025 客戶滿意度調查

橘子以提升服務品質與客戶體驗爲核心，透過 AI 智能技術、數據分析與標準化作業流程，強化客服整體應對能力。爲提升首次回應解決率與服務正確率，本公司持續優化客服作業流程，結合 AI 客服、智能分流機制與知識庫應用，強化前線即時判斷與回應能力。同時，透過 AI 輔助文本生成工具與品質檢測機制，提升回覆一致性與資訊準確性，並搭配定期教育訓練與品質稽核，確保服務標準落實。在應對大量問題與降低重複客訴方面，橘子持續深化數據分析與自助化服務應用。透過即時掌握高頻問題與用戶需求趨勢，動態優化 FAQ 與 AI 客服語料，提升自助服務解決能力；並結合前端攔截（如公告提示、BOT 引導）與批次回覆機制，降低重複進件與回覆負擔；同時搭配一站式自助服務與流程自動化，強化整體服務效率與營運韌性。

整體而言，透過 AI 技術導入、數據驅動管理與自助服務優化，持續提升服務效率與品質穩定度，並在面對服務量波動時仍能維持一致且高品質的客戶體驗，進一步強化品牌信任與用戶忠誠度，作爲企業永續發展之重要基礎。

### 2025 客戶服務亮點

| 項目 | 2025 年 |
|---|---|
| 年服務量 | 19 萬 |
| 客戶滿意度 | 4.77 |
| 首次回應達成率 | 92.1% |
| 服務品質檢測正確率 | 99.6% |

註：1. 客戶滿意度使用 5 分量表。
2. 服務品質檢測正確率係指客服中心於一定期間內，針對各類服務互動進行抽樣檢測後，符合服務標準之案件比例。該指標可反映客服人員對產品知識、流程規範、資訊提供的正確掌握度，同時亦可作爲評估訓練成效、知識庫維護、系統輔助程度的指標。通過設置明確的評核標準與錯誤定義，導入評分表（Scorecard）進行標準化記錄，利用風險類型區分、AI 質檢輔助等分層檢測機制，並結合教育訓練及應用改善措施，實現服務品質檢測循環，確保服務品質不斷完善及提升。

## 客戶滿意度行動方案

針對重大申訴或潛在安全風險案件，本公司設有專責處理小組，即時啟動跨部門協調機制，確保調查、溝通與回覆流程符合主管機關規範並準時完成。

針對客戶申訴與政府機關來函，橘子依循標準化處理流程與法規要求，由專責單位統一受理與追蹤，並透過跨部門協作機制進行調查與回應，確保所有案件均於 15 日內完成處理與回覆。2025 年共接獲政府機關來函 513 件，其中 85 件需召開協調會，均依規定於 15 日內完成回覆，準時回應率達 100%。2025 年未發生重大資安、隱私洩漏或政府列管事件，持續維護企業形象與社會信任。客訴案件仍以新楓之谷產品爲主，經分析主要集中於帳號管理與活動機制相關議題，反映用戶對公平性、資訊透明度與資安保障之高度關注。
主要樣態如下：

| 主要客訴樣態 | 占比 | 處理方式 |
|---|---|---|
| 帳號限制 / 停權 | 42% | 針對疑似違規或外掛行爲，啟動內部複查機制，經營運判定違規屬實者，維持帳號限制措施，以確保平台公平性與使用秩序。 |
| 活動爭議 / 退費 | 31% | 針對活動設定調整或流程未臻完善所衍生之爭議，透過統一補償機制處理，並開設專案服務管道（如 LINE 官方帳號），提供即時且一對一之溝通與說明，降低客訴影響。 |
| 帳號遭盜用 | 8% | 提供專案服務協助追蹤虛擬資產流向，已追回之資產歸還用戶；未追回部分依定型化契約處理，並協助用戶了解後續法律求償途徑。 |

### 後續行動方案

本公司持續以主管機關來函案件爲重要優化依據，透過制度與科技並行的方式，強化風險控管與服務品質，降低類似客訴發生。2025 年重點優化方向包括：

1. **深化數據分析與根因管理：**定期彙整客訴類型與關鍵成因，回饋產品設計與營運策略調整。
2. **強化跨部門應變機制：**優化爭議案件處理流程，由產品、營運、法務與客服單位協同應對，提升處理效率與一致性。
3. **優化服務與溝通機制：**透過專案服務管道與即時回應機制，提升資訊透明度與用戶理解。
4. **提升資安防護與用戶教育：**持續推廣帳號管理安全機制，降低帳號遭盜風險。

透過上述措施，本公司逐步強化以預防爲導向之客訴管理機制，提升顧客信任與服務品質，並持續落實企業對消費者權益保障與社會責任之承諾。