又一村花園俱樂部有限公司
資料外洩事故的調查報告

根據香港法例第 486 章《個人資料（私隱）條例》第 48(2)條發表

背景

個人資料私隱專員公署（私隱專員公署）已就又一村花園俱樂部有限公司（又一村花園俱樂部）通報的一宗資料外洩事故完成調查。

調查源於又一村花園俱樂部於 2025 年 10 月 31 日向私隱專員公署通報的資料外洩事故。事故涉及又一村花園俱樂部存放於伺服器內的俱樂部管理系統檔案遭勒索軟件加密而無法運作（外洩事件）。

有關的俱樂部管理系統負責管理俱樂部的會員資料，而所有相關的個人資料均儲存於上述伺服器內，並由外判服務供應商負責提供及維護系統，服務供應商會透過專用的遠端存取軟件連接伺服器，以提供技術支援。

調查發現，事發時相關遠端存取軟件屬已過時版本，並存在已知的保安漏洞。黑客利用該漏洞成功竊取服務供應商的帳戶憑證，從而直接進入儲存大量個人資料的相關伺服器。此外，該伺服器長時間保持登入狀態，俱樂部並無實施額外的身分認證措施，進一步削弱系統的保安防護。同時，俱樂部的防毒軟件及防火牆均已過時，未能偵測及阻止黑客活動。

又一村花園俱樂部為一所私人、非牟利的社交及康樂機構，專門為已登記會員及賓客提供康樂設施及餐飲服務。外洩事件合共影響 9,045 名資料當事人，包括 1,553 名活躍會員、1,723 名附屬卡持有人、1,313 名前會員，以及 4,456 名前附屬卡持有人。受影響的個人資料包括姓名、香港身份證號碼及／或護照號碼、出生日期、電郵地址、聯絡電話及地址。

在外洩事件發生後，又一村花園俱樂部已通知受影響的人士，並採取多項補救措施，包括停止使用存在漏洞的遠端存取軟件、對所有遠端存取連接進行監控、將所有伺服器及端點的防毒軟件及防火牆更新至最新版本，以及將儲存於伺服器內的個人資料檔案加密。

調查結果

私隱專員公署就外洩事件共進行了四次查訊，並審視了俱樂部提供的資料，以及俱樂部就外洩事件的跟進及補救工作。經考慮外洩事件的情況及調查所獲得的資料，個人資料私隱專員（私隱專員）鍾麗玲認為又一村花園俱樂部的以下缺失是導致外洩事件發生的主因（詳見附件一）：—

1. 使用已過時並存在保安漏洞的遠端存取軟件；
2. 伺服器的遠端存取欠缺用戶身分認證措施；
3. 使用已過時的防毒軟件及防火牆；
4. 欠缺資訊保安的機構性措施；及
5. 過長地保留個人資料。

私隱專員的決定

又一村花園俱樂部在外洩事件發生前，未有採取適當及充分的機構性及技術性資訊保安措施，以保障其資訊系統內所儲存的個人資料，私隱專員對此表示失望。基於上述情況，私隱專員裁定又一村花園俱樂部沒有採取所有切實可行的步驟以確保涉事的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，因而違反了《個人資料（私隱）條例》（《私隱條例》）的保障資料第 4(1)原則有關個人資料保安的規定。

此外，私隱專員認為又一村花園俱樂部沒有採取所有切實可行的步驟，以確保個人資料的保存時間不超過使用相關資料實際所需的時間，因而違反了《私隱條例》的保障資料第 2(2)原則有關個人資料保存期限的規定。

私隱專員已向又一村花園俱樂部送達執行通知，指示其採取措施以糾正違規事項，以及防止類似違規情況再次發生。

建議

私隱專員希望藉此報告，建議機構應採取足夠及合適的機構性及技術性措施，以保障載有個人資料的資訊系統，包括：

- 及時更新遠端存取軟件、防毒軟件及防火牆，以修補已知漏洞；
- 為存取資料實施有效的用戶身分認證，包括使用強密碼及多重身分認證；
- 建立充分的機構性措施，包括資訊保安的內部政策及穩妥的遠端存取方案；
- 定期進行保安風險評估、漏洞掃描及系統審計，以識別並修補保安弱點；
- 制定資料保留政策，確保個人資料不會被不必要地保留；及
- 為員工提供定期資訊保安培訓。

鍾麗玲
個人資料私隱專員
2026 年 4 月 23 日

附件一

又一村花園俱樂部有限公司資料外洩事故
導致發生資料外洩事故的缺失

1. **使用已過時並存在保安漏洞的遠端存取軟件**：又一村花園俱樂部用於遠端存取的軟件於事發時屬已過時版本，並存在已知的保安漏洞，黑客利用該漏洞發動勒索軟件攻擊。調查發現，相關軟件開發商早於2025 年 1 月已發出保安警報，提醒受影響的用戶，惟服務供應商並不知悉有關警報。此外，又一村花園俱樂部及服務供應商均未有就相關軟件建立任何保安更新或修補機制；

2. **伺服器的遠端存取欠缺用戶身分認證措施**：又一村花園俱樂部刻意將存放伺服器的電腦長時間維持於登入狀態，確保用於遠端存取的軟件可持續在背景運行，令服務供應商毋須額外認證便可進行遠端存取。俱樂部表示，相關做法基於操作便利及沿用舊有操作，以便服務供應商能即時提供遠端技術支援。惟於外洩事件發生時，該軟件並未具備多重認證功能，致使黑客能在毋須進一步認證的情況下，憑藉已竊取的憑證經該軟件進入系統；

3. **使用已過時的防毒軟件及防火牆**：由於維護周期出現疏漏，相關伺服器上啟用的防火牆已屬過時，因而限制俱樂部偵測及阻截黑客活動的能力。俱樂部亦承認，其防毒軟件同屬過時，導致於外洩事件中未能偵測到任何與勒索軟件相關的警報；

4. **欠缺資訊保安的機構性措施**：又一村花園俱樂部在外洩事件前並未制定任何書面的資訊保安政策或指引。雖然俱樂部曾與服務供應商簽訂有關俱樂部管理系統及伺服器技術支援的服務合約，但該合約並未就資訊保安訂明任何明確要求。俱樂部亦未能證明其已採取任何有效的機構性措施，以保障相關伺服器或儲存在內的個人資料安全；及

5. **過長地保留個人資料**：基於法定財務紀錄保存要求，以及查核會員復會申請及處理過往帳單爭議的需要，又一村花園俱樂部於會員或附屬卡持有人取消會籍後，最少保留其個人資料七年。然而，調查發現，又一村花園俱樂部保留了 888 名前會員及 3,321 名前附屬卡持有人的個人資料，而相關保存時間均已超過七年。