COUNTRY GARDEN SERVICES HOLDINGS COMPANY LIMITED
碧桂園服務控股有限公司

(於開曼群島註冊成立之有限公司)
(股份代號：6098.HK)

信息安全管理政策

1. 總則

碧桂園服務控股有限公司（簡稱「碧桂園服務」或「集團」）為全面規範集團信息安全管理工作，健全統一、動態迭代的信息安全防護體系，保障集團網絡、軟硬件系統、業務數據、客戶信息、辦公資產全維度安全，前置防範各類網絡攻擊、數據洩露、系統故障等安全風險；同時清晰界定內部員工、第三方合作方的信息安全權責，建立長效、閉環的安全管控機制，穩定支撐集團經營，依據國家網絡安全、個人信息保護相關法律法規，結合集團業務實際，特制定本政策。

2. 適用範圍

集團及其子集團和分支機構的全部運營活動下的所有用工應遵循本政策。

3. 管理原則

集團信息安全管理遵循「安全第一、預防為主、動態完善、全程管控、權責明確、全員負責」的原則，堅持系統建設與日常運維相結合、風險監控與應急處置相結合、內部管控與第三方約束相結合，全方位保障集團信息安全。

4. 管理組織架構與崗位職責

本集團構建信息安全組織架構。由集團首席技術官（CTO）及各部門總經理組成信息安全領導小組，統籌信息安全、個人信息保護管理事項，審批相關戰略、年度計劃與重大投入，開展工作監督；信息安全團隊負責落實各項管控策略及日常運營。

5. 信息安全系統建設與動態完善

5.1 安全系統迭代完善機制：集團建立信息安全系統常態化完善機制，結合業務迭代、新型網絡風險及合規要求，持續優化網絡、安全、權限、審計、備份等安全系統能力，杜絕安全體系滯後於業務發展。

5.2 常態化整改優化：定期開展安全自查、漏洞掃描、配置核查，及時完成系統升級、補丁更新、策略優化、隱患整改。針對新場景、新設備、新系統上線，同步配套安全防護策略，持續補齊安全短板，保障安全體系持續有效、適配業務發展。

6. 數據安全與完整性保護

6.1 數據分級分類管理：集團數據分為公開數據、內部數據、普通商業機密、核心商業機密四級，實行分級授權、分級防護、分級留存管理。嚴格執行最小權限原則，按需分配數據訪問、操作、導出權限，杜絕超權限使用數據。

6.2 數據完整性保護要求：所有業務數據、檔案資料必須真實、準確、完整，嚴禁私自篡改、偽造、刪除、覆蓋有效數據。系統開啟操作日誌、數據校驗、防篡改機制，確保數據變動全程留痕、可追溯。

6.3 數據保密要求：嚴禁私自導出、外傳、截圖、拷貝敏感及核心數據，禁止將集團涉密數據留存至個人終端、網盤、手機等私人設備。人員調崗、離職必須全數回收權限、清理個人留存數據。

7. 信息安全威脅監控與應急處置

7.1 安全威脅監控：技術團隊對集團網絡、系統登錄、終端行為、數據操作、異常訪問實行常態化監控，實時識別病毒木馬、網絡攻擊、異常批量導出、異地異常登錄、違規接入等安全威脅，做到早發現、早預警、早處置。

7.2 安全事件應急處置流程：發生信息洩露、系統異常、網絡攻擊、病毒入侵、數據丟失等安全事件時，相關人員須第一時間上報。技術部門立即啟動應急處置，採取隔離風險、封堵漏洞、凍結權限、溯源核查等措施，控制風險擴散，事後完成覆盤整改，優化防護策略。

7.3 風險排查與隱患整改：定期開展安全隱患排查，重點核查賬號安全、終端安全、網絡邊界、系統漏洞、數據傳輸等關鍵環節，建立隱患台賬，實行閉環整改，降低常態化安全風險。

8. 員工信息安全個人責任

8.1 全員安全責任要求：所有員工為本崗位信息安全第一責任人，對本人操作行為、賬號安全、經手數據安全承擔直接責任，嚴格遵守集團信息安全管理制度，主動防範崗位安全風險。

8.2 責任追究機制：因個人違規操作、疏忽履職、故意洩密等行為造成系統故障、數據洩露、財產及聲譽損失的，集團將視情節給予通報、績效處罰、崗位調整，情節嚴重的依法追究法律責任。

9. 第三方合作單位信息安全管理要求

9.1 第三方準入安全要求：本條款適用所有為集團提供技術開發、運維服務、設備供應、諮詢服務、外包服務等各類第三方供應商、合作單位。所有第三方合作主體在合作準入前，必須接受集團信息安全資質審核，提交安全承諾書，明確合作期間信息安全責任，未通過安全審核的，不得開展合作。

9.2 第三方合作安全約束

a. 第三方接入集團網絡、系統及接觸數據，僅限業務必要場景，最小權限使用，嚴禁超範圍操作、留存、拷貝集團數據；

b. 第三方人員操作全程登記、行為留痕，接受集團安全監督檢查；

c. 嚴禁第三方篡改、洩露、倒賣、外傳集團業務及客戶數據；

d. 第三方須自行做好自身設備與人員安全防護，因第三方原因造成的安全事故，由第三方承擔全部責任。

10. 個人信息合規審計管理

10.1 個人信息審計是指對集團各實體個人信息安全合規性、有效性進行定期分析。

10.2 為持續保障集團業主個人信息全流程合規，集團建立常態化合規審計機制，開展內部合 規審計工作。相關工作包括開展風險評估，核查是否存在個人信息安全漏洞、個人信息保護與隱私管理制度合規性，以及集團下屬各單位個人信息安全管控措施落實成效。

10.3 企業在一定情形下應委託專業機構，每兩年至少開展一次個人信息保護合規審計，以評估集團各實體的合規有效性並提供證據證明集團各實體的個人信息安全合規性。

11. 培訓、監督與考核

11.1 安全培訓教育：常態化開展信息安全培訓、警示教育及應急演練，強化全員安全意識，提升風險識別與處置能力。新員工必須完成入職信息安全培訓後方可上崗。

11.2 考核獎懲機制：信息安全工作納入個人考核。對有效規避重大風險、排查重大隱患的予以表彰；對履職不到位、違規操作造成安全問題的嚴肅追責。

12. 政策審視與修訂

本政策經公司董事會審議批准，並由集團信息安全領導小組監督其有效實施。爲確保本政策持續適應外部監管環境變化及公司內部管理需要，集團信息安全領導小組將適時對本政策的適用性及有效性進行審視及檢討，並結合檢討結果、法律法規更新評估考量是否修訂本政策，報董事會最終審批。