惠生工程技術服務有限公司

信息安全管理說明

一、目的與適用範圍

惠生工程技術服務有限公司（“惠生工程”或“本公司”）重視信息、數據、工程設計成果、客戶資料和信息系統的安全。《信息安全管理說明》（“本說明”）描述本公司建立簡明、可執行的信息安全框架，以保護本公司信息的機密性、完整性和可用性，並支持業務持續運營。

本說明適用於惠生工程，並概述本公司推動其具有運營控制權的附屬公司開展信息安全管理的總體原則。各附屬公司根據其業務性質、適用法律法規、公司的運營控制程度及現有管理體系落實相關要求。本公司亦對在適用情況下接觸公司信息或系統的承包商、顧問、供應商及其他業務夥伴提出相應的信息安全要求。

二、信息安全承諾

- 持續改進：通過評估、培訓、檢查、事件複盤和整改跟蹤，持續提升信息安全管理。
- 信息保護：按照信息敏感程度實施分類保護，防止未經授權的訪問、披露、篡改、丟失或破壞。
- 威脅監測與響應：採取適當措施預防、監測和應對惡意軟件、網絡攻擊、信息誤發、異常訪問及其他安全威脅。
- 員工責任：員工應遵守信息安全要求，保護賬號、設備和本公司信息，並及時報告可疑事項。
- 第三方要求：對接觸本公司信息或系統的重要第三方開展適當安全評估，並通過合同明確保密、訪問控制和事件通知要求。

三、主要管理方案

3.1 風險與漏洞管理

本公司至少每年開展一次信息安全風險評估，並在重大系統上線、重大變更、重要第三方接入或重大事件後按需要更新。本公司定期識別系統弱點，優先處理高風險漏洞；如無法於短期內修復的，應採取臨時緩解措施並跟蹤關閉。

3.2 信息分類與訪問控制

本公司按照信息敏感程度實施分類保護，並按照最小權限原則審批和定期複核訪問權限。員工調崗或離職時，應及時調整或撤銷權限。

3.3 業務連續性

本公司識別關鍵業務和系統，制定必要的備份、恢復及替代作業安排。關鍵業務連續性或恢復安排至少每年進行一次測試或演練，並對發現的問題進行整改。

3.4 信息安全事件報告與升級

員工及相關外部人員發現可疑郵件、設備遺失、信息誤發、異常訪問、惡意軟件或其他潛在事件時，應立即向信息技術部門或指定信息安全負責人報告。本公司根據事件嚴重程度開展記錄、評估、控制、修復和恢復，並在必要時把事件升級至管理層、法律合規部門及董事會或其授權委員會。本公司依法依約評估並履行適用的外部通知義務。

3.5 培訓與意識

本公司向員工提供入職及年度信息安全培訓，內容包括賬號保護、網絡釣魚、信息分類、設備及移動辦公安全、數據處理和事件報告。

3.6 內部檢查

本公司至少每年開展一次內部信息安全檢查或審閱。發現問題應明確責任人、整改措施和完成日期，並跟蹤至關閉。本公司可根據風險和業務需要安排獨立第三方評估。

四、治理與職責

本公司行政總裁負責監督本公司重大信息安全風險和事宜及負責本公司信息安全戰略審議。數字化部負責應用安全及運維安全等信息安全的管理。

五、批准與複審

本說明由本公司管理層批准，自公開發布之日起生效。本公司至少每年複審一次，並在法律監管、組織架構、業務模式、重要技術或威脅環境發生重大變化時及時更新。