

信息安全管理说明

一、目的与适用范围

惠生工程技术服务有限公司（“惠生工程”或“本公司”）重视信息、数据、工程设计成果、客户资料和信息系统的安全。《信息安全管理说明》（“本说明”）描述本公司建立简明、可执行的信息安全框架，以保护本公司信息的机密性、完整性和可用性，并支持业务持续运营。

本说明适用于惠生工程，并概述本公司推动其具有运营控制权的附属公司开展信息安全的总体原则。各附属公司根据其业务性质、适用法律法规、公司的运营控制程度及现有管理体系落实相关要求。本公司亦对在适用情况下接触公司信息或系统的承包商、顾问、供应商及其他业务伙伴提出相应的信息安全要求。

二、信息安全承诺

- 持续改进：通过评估、培训、检查、事件复盘和整改跟踪，持续提升信息安全管理。
- 信息保护：按照信息敏感程度实施分类保护，防止未经授权的访问、披露、篡改、丢失或破坏。
- 威胁监测与响应：采取适当措施预防、监测和应对恶意软件、网络攻击、信息误发、异常访问及其他安全威胁。
- 员工责任：员工应遵守信息安全要求，保护账号、设备和本公司信息，并及时报告可疑事项。
- 第三方要求：对接触本公司信息或系统的重要第三方开展适当安全评估，并通过合同明确保密、访问控制和事件通知要求。

三、主要管理方案

3.1 风险与漏洞管理

本公司至少每年开展一次信息安全风险评估，并在重大系统上线、重大变更、重要第三方接入或重大事件后按需要更新。本公司定期识别系统弱点，优先处理高风险漏洞；如无法于短期内修复的，应采取临时缓解措施并跟踪关闭。

3.2 信息分类与访问控制

本公司按照信息敏感程度实施分类保护，并按照最小权限原则审批和定期复核访问权限。员工调岗或离职时，应及时调整或撤销权限。

3.3 业务连续性

本公司识别关键业务和系统，制定必要的备份、恢复及替代作业安排。关键业务连续性或恢复安排至少每年进行一次测试或演练，并对发现的问题进行整改。

3.4 信息安全事件报告与升级

员工及相关外部人员发现可疑邮件、设备遗失、信息误发、异常访问、恶意软件或其他潜在事件时，应立即向信息技术部门或指定信息安全负责人报告。本公司根据事件严重程度开展记录、评估、控制、修复和恢复，并在必要时把事件升级至管理层、法律合规部门及董事会或其授权委员会。本公司依法依约评估并履行适用的外部通知义务。

3.5 培训与意识

本公司向员工提供入职及年度信息安全培训，内容包括账号保护、网络钓鱼、信息分类、设备及移动办公安全、数据处理和事件报告。

3.6 内部检查

本公司至少每年开展一次内部信息安全检查或审阅。发现问题应明确责任人、整改措施和完成日期，并跟踪至关闭。本公司可根据风险和业务需要安排独立第三方评估。

四、治理与职责

本公司行政总裁负责监督本公司重大信息安全风险和事宜及负责本公司信息安全战略审议。数字化部负责应用安全及运维安全等信息安全的管理。

五、批准与复审

本说明由本公司管理层批准，自公开发布之日起生效。本公司至少每年复审一次，并在法律监管、组织架构、业务模式、重要技术或威胁环境发生重大变化时及时更新。