香港中华煤气有限公司

附录 15：信息保安政策

我们的目的

本政策规定了香港中华煤气有限公司（「本公司」）及其附属公司（统称「中华煤气集团」）的责任和政策，确保中华煤气集团信息和技术资产的机密性、完整性和可用性。我们鼓励所有项目公司、联营公司、 供货商和业务伙伴在适用的情况下参考本政策的原则。

我们的承诺

信息是公司极具价值和重要的资产，须防范可能对其机密性、完整性和/或可用性受威胁的风险。有效的信息安全管理能够在信息共享的同时将其所面临的风险减到最低。 我们将不断改进信息安全系统，以助监控和应对信息安全威胁。

根据 ISO/IEC 27002 国际信息安全管理标准，中华煤气集团承诺：

- 保障中华煤气集团资产能得到适当的等级保护并问责；
- 确保雇员、承包商和第三方用户了解他们的责任和信息安全要求，及符合他们所担当角色的相关要求，以帮助降低被盗窃、欺诈或滥用设施的风险；
- 降低在正常工作时间内外信息遭到未经授权访问、丢失和损坏的风险；
- 透过意识培训，确保正确利用任何计算机、网络、移动设备、电话、电子邮件、实时通信服务、社交网站、语音邮件和传真来开展内部和对外业务；
- 保护中华煤气集团的知识产权，包括商标、版权和商业秘密，免遭滥用和未经授权的披露；
- 监管中华煤气集团外部的供货商、顾问、承包商和其他服务提供商的选择和管理，并保护中华煤气集团的信息及其处理设施；
- 制定一份记录在案并通过测试的灾难复原计划管理文档，描述当在关键系统因灾难中断影响运营的情况下，如何确保仍可继续营运业务；
- 保护客户信息；
- 确保采用适当的用户授权访问信息系统及妥善维护帐户；
- 制定使用移动设备访问中华煤气集团资源的可接受范围；
- 实施控制措施限制授权人员访问信息处理设施，同时提供正常业务活动中断期间的监控；
- 监控外网远程访问系统；
- 确保按照业务和安全的基本要求控制对网络、服务和信息系统的访问，同时权限需得到适当授权、分配和维护，严禁未经授权的访问；
- 建立创建强密码、密码保护以及更改频率的标准；
- 最低安全风险实践贯穿于系统需求收集、开发和维护整个过程中，以确保所有

信息系统得到足够安全保护，并防止应用程序使用中出现错误、丢失、未经授权的修改或误用；

- 以合理及可预见的方式管理对生产服务器、设施、应用程序、网络和基础设施服务的更新修改，以便雇员和用户能够做出有计划的应对，从而降低未经授权此类更新修改与错误造成系统服务中断的可能性；
- 为已经得到公众认可并证明有效的加密算法提供使用指引，提供管理加密密钥方向，并确保遵守有关使用加密技术的适用规则；
- 确保信息备份足以覆盖大部分可预期情况，以尽量把丢失数据和影响操作减到最小；
- 制定使用的网络设备、服务器和应用程序的补丁管理和技术更新的基线要求，将潜在漏洞的风险降至最低；
- 制定检测、预防和恢复流程，防止在中华煤气集团拥有或管理的用户终端设备（如已派发的工作站、笔记本电脑和移动设备）以及 IT 基础设施网络和系统上执行恶意软件；
- 通过采用云服务商提供的安全保护服务与措施，保障云端应用系统安全且高效；
- 确保对煤气公司面向互联网的网络资源和面向客户的网络应用程序得到适当的保护；
- 确保对煤气公司的机密数据按照分类级别进行适当的泄漏预防保护;
- 制定应用程序 API 接口的管理, 包括接口验证及数据加密保护措施等;
- 确保人工智能用得其所符合中华煤气集团利益及数据安全;
- 确保物联网设备开发及应用，融入风险考虑因素及保护措施，减少网络攻击风险；及
- 确保特权账号的访问控制仅限于具有合理业务需求的账户，包括对特权账户的申请、审批、记录、检视及设置密码的要求。

针对我们的信息安全要求和考虑已制定了一套内部政策。

更新日期：2024 年 8 月 30 日