APPENDIX 15: INFORMATION SECURITY POLICY

Our Purpose

This policy sets out the obligations and policies of The Hong Kong and China Gas Company Limited (the "Company") and its subsidiaries (collectively the "Group") to ensure the confidentiality, integrity and availability of the Group's information and technology assets. All our project companies, associates, suppliers and business partners are encouraged to make reference to the principles of this policy, where applicable.

Our Commitment

Information is an extremely valuable and important corporate asset that requires protection against risks that would threaten its confidentiality, integrity and/or availability. Effective information security management enables information to be shared while minimising its exposure to risk.

Aligned with ISO/IEC 27002, an international information security management standard, the Group is committed:

- To help ensure appropriate level of protection and accountability of the Group assets;
- To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to help reduce the risk of theft, fraud or misuse of facilities;
- To reduce the risks of unauthorised access, loss of, and damage to information during and outside normal working hours;
- To ensure proper use of any computer, network, mobile devices, telephone, electronic mail, instant messaging, social networking websites, voice mail, and facsimile to conduct business both internally and externally;
- To protect intellectual property portfolio of the Group, including trademarks, copyrights, and trade secrets, from misuse and unauthorised disclosure;
- To govern the selection and administration of vendors, consultants, contractors and other service providers external to the Group, and to protect the Group information and processing facilities;
- To have a documented and tested Business Continuity Plan that describes how business will be conducted if critical systems are disrupted by a disaster affecting operations;
- To protect customer information;
- To ensure proper user authorisation and account maintenance for accessing information technology services of the Group;
- To outline the acceptable use of mobile devices to access the Group resources;
- To implement control to restrict access to the information processing facilities to authorised personnel and to provide control over the disruption of normal business activities;
- To control external remote access to systems under the administration of the Group;
- To ensure that access to networks, services and information systems are controlled on the basis of business and security requirements, and that the access rights are appropriately authorised, allocated and maintained, and unauthorised access is prohibited;
- To establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change;
- To specify the minimum security practices during system acquisition, development and maintenance processes, in order to ensure sufficient security in all information systems, and prevent errors, loss, unauthorized modification or misuse of information in applications;
- To manage changes to production servers, facilities, applications, networks and infrastructure services in a rational and predictable manner so that staff and users of the Group can plan accordingly, and to minimise the likelihood of disruption, unauthorized alterations and errors;

- To provide guidance on the use of encryption algorithms that have received public review and have been proven to work effectively, and provide direction on managing cryptographic keys and ensures that applicable regulations on the uses of cryptographic technology are followed;
- To ensure the information backups are adequate to cover most of the pre-defined case in order to minimise any data loss and impact to operation;
- To specify the baseline requirements on patch management and technology refreshment on network equipment, servers and applications used, and to help minimise the risk of successful vulnerability exploitation;
- To standardise the detection, prevention and recovery controls to prevent the execution of malware on the Group Towngas owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components;
- To make cloud application use safe and productive by adopting the Cloud Access Security Broker strategy for application protection;
- To help ensure appropriate level of protection of Towngas internet facing network resources and customer facing web applications;
- To help ensure appropriate level of data leakage prevention protection of Towngas classified information;
- To develop Application Programming Interface ("API") management, including interface authentication and data encryption protection measures;
- To ensure the appropriate use of artificial intelligence ("AI") that aligns with the Group's interests and data security;
- To ensure the development and application of Internet of Things ("IoT") devices incorporate risk considerations and protection measures to reduce the risk of cyber attacks;
- To ensure access control to privileged accounts is limited to those with a justifiable business requirement, with requirements of application, approval, record-keeping, review, and secure password for privileged accounts.

A set of in-house policies has also been developed for our information security requirements and considerations.

Date of last update: 30 August 2024