港燈電力投資
HK Electric Investments

Information Security Policy

August 2021

Table of Contents

1 Introduction

1.1 HK Electric Investments Limited and its subsidiaries including The Hongkong Electric Company, Limited (collectively, the "Group") takes information security very seriously. Information resources within the Group (the "information assets" or "information"), regardless of the form they exist and how they are created, distributed, used, or stored, are valuable assets and must be protected from unauthorised access, modification, deletion, or disclosure, either intentionally or accidentally.

1.2 This Policy, being the overarching policy for information security, outlines the approach, methodology, responsibilities, and requirements for protecting information while enabling the effective and appropriate use of information in the course of conducting the Group's business and technical operations.

1.3 This Policy is the backbone of the Group's information security governance framework within which a set of issue-specific security policies, standards, guidelines, and procedures have been developed to address the following three key requirements of information security:

- **Confidentiality**: Protecting information from unauthorised access or disclosure. Access to information shall be confined to authorised individuals on a need-to-know basis.
- **Integrity**: Safeguarding information from any unauthorised modification or deletion to ensure its accuracy, completeness, and validity.
- **Availability**: Ensuring information is accessible only by those authorised individuals as and when required.

2 Scope

2.1 This Policy applies to:

2.1.1 All employees across the Group, contractors, and suppliers who are granted access to the Group's premises, systems, or information (the "users").

2.1.2 All information systems and technology platforms within the Group (the "IT facilities"), and information on those systems and platforms, related electronic media, or printouts.

3 Objectives

3.1 This Policy aims to protect information assets and IT facilities from all security threats and vulnerabilities, whether internal or external, malicious, or accidental. The

objectives of this Policy are to:

3.1.1 Define the principles and requirements of acceptable use of information and IT facilities and describe how these should be implemented across the Group.

3.1.2 Establish the Group's information security governance framework, based on ISO/IEC 27002:2013 – Code of Practice for Information Security Controls, for:

3.1.2.1 Helping users understand the Group's expectation and requirements for acceptable use of information and IT facilities, and their roles and responsibilities in protecting the confidentiality, integrity, and availability of information.

3.1.2.2 Implementing appropriate controls, processes, and technologies following various issue-specific security policies, standards, and guidelines for safeguarding information assets commensurate with their respective levels of sensitivity and value.

3.1.3 Raise the level of information security awareness among users.

4 Organisational Roles and Responsibilities

4.1 Information security and the appropriate protection of information are the responsibilities of all users. Individuals are always expected to act professionally and responsibly while conducting business. Users are accountable for their actions concerning the use of information and, if applicable, the associated IT facilities. This section describes the different areas of roles and responsibilities for ensuring that information and the related IT facilities remain secure.

4.2 General Manager (Information Technology)

4.2.1 The General Manager (Information Technology) has direct responsibilities for:

4.2.1.1 Managing the development, implementation, and maintenance of this Policy.

4.2.1.2 Taking ownership of information security governance and managing the development, implementation, and maintenance of issue-specific security policies, standards, guidelines, and procedures to ensure the security of information assets and the associated IT facilities.

4.2.1.3 Managing major information security projects and monitoring information security assessments throughout the Group.

4.2.1.4 Reviewing and, if necessary, revising existing or implementing new measures to

ascertain the security of information and IT facilities from time to time.

4.2.1.5 Establishing information security risk assessment guidelines and reporting mechanism to help different business units throughout the Group conduct security risk assessment and report information security status and significant security matters within their respective areas of responsibilities.

4.2.1.6 Developing compliant procedures, processes, and practices for the use of IT facilities and information.

4.2.1.7 Serving as the focal point for handling security incidents and providing information security advice and assistance to various business units on trends and threats of information security that may affect the Group.

4.2.1.8 Devising a strategy for and implementation of information security awareness education programs for the Group.

4.2.1.9 Reviewing the effectiveness of this Policy at least once a year and, if appropriate, making necessary changes to the Policy to reflect the current state of the business and regulatory requirements as well as to combat the growing number and wider variety of information security threats and vulnerabilities.

4.3 Business Unit Heads

4.3.1 Business unit heads are directly responsible for full compliance with this Policy and relevant issue-specific security policies, guidelines, and procedures within their respective business areas. Specifically, business unit heads are responsible for:

4.3.1.1 Ensuring that all their employees and relevant contractors are fully conversant with this Policy and all associated issue-specific policies, standards, guidelines, procedures, and applicable legislation and are aware of the consequence of non-compliance.

4.3.1.2 Providing appropriate training to their employees and contractors for using the Group's IT facilities and information assets.

4.3.1.3 Serving as information owner(s) for information assets within their respective areas of responsibilities.

4.3.1.4 Managing information risk as part of their wider risk management responsibilities through regular risk assessment and reporting.

4.3.1.5 Implementing appropriate measures within their respective business areas to

minimise the Group's exposure to information risk. Such measures may include business continuity plans, segregation of duties, dual control, or job rotation in critical susceptible areas.

4.3.1.6 Notifying Information Technology Division ("IT") via established procedures of any changes of employee's job function or status due to job rotation, promotion, or resignation that may affect access rights to information. The same principle also applies to contractors or others who have access to information to perform their duties. Likewise, notifying IT or relevant information owner of any suspected or actual breaches, or perceived weaknesses of information security.

4.4 Internal Audit

4.4.1 Internal Audit is responsible for conducting information security audits to check compliance with policies and guidelines.

4.5 The Users

4.5.1 The Group's IT facilities and information assets are provided for and must be used only for business purposes. Users may access, use, or share information only to the extent it is authorised and necessary to perform their assigned job duties. The use of such assets imposes certain responsibilities and obligations on users and is subject to all applicable Group policies and guidelines. In this connection, users are responsible for the following concerning information security:

4.5.1.1 Ensuring that information assets and IT facilities are not misused, and conforming to all Group security policies, standards, guidelines, and procedures.

4.5.1.2 Reporting all real or suspected information security incidents such as the theft, loss, or unauthorised disclosure of information, or any perceived weakness in the Group's security policies, processes, or infrastructure to the General Manager (Information Technology), via established procedures, or their business unit head as appropriate. For contractor users, security incidents including, but not limited to, crimes, threats, breaches of security, and other irregularities shall be reported to the designated Group personnel.

4.6 Information Owners

In the context of this Policy, information owners are individual business unit heads within the Group or his/her designated representative(s) who make decisions on who has the right to access the information and how it shall be managed and used throughout its lifecycle. However, under all circumstances, business unit heads retain accountability and must ensure that appropriate security measures are in place to

protect the confidentiality, integrity, and availability of the information they own.

4.6.1 In the context of information security, the information owner is responsible for:

4.6.1.1 Ensuring that information is classified according to the Group Information Classification Policy and appropriate security controls are in place to guard against unauthorised access, disclosure or modification.

4.6.1.2 Communicating classification (i.e. "Unclassified", "Internal Use Only", or "Confidential") of information when it is released to other business units within the Group or other external third parties.

4.6.1.3 Controlling access to information based on the principle of least-privilege and need-to-know, and granting users only the rights and permissions they need to perform their job.

4.6.1.4 Reviewing the access rights associated with information assets on a regular basis, and making necessary amendments as and when appropriate.

5 Information Security Risk Management

5.1 To effectively manage information risks, each risk must be identified and assessed through a formal risk assessment. The Group has adopted a practice of conducting group-wide assessment to identify new and pertinent information security risks, and devise recommendations for optimising information security by implementing suitable controls and other risk mitigation actions based on vulnerabilities and impact on information and IT facilities.

6 Appropriate Use

6.1 Information and IT facilities shall be used for business purposes or other approved activities. The Group reserves the right to inspect and/or disclose all information stored in or transmitted over IT facilities without the consent of any of the users. However, such inspection will only be performed to assure compliance with internal policies, to support internal compliance or fraud investigations, to comply with legal requirements such as a subpoena or court order, or to assist with the management of IT facilities. Such inspection will only be carried out with the authorisation of the Business Unit Head of the concerned user and witnessed by a representative of the business unit.

7 Information Classification Management

7.1 Information assets must be categorised into different classifications to reflect their

respective levels of sensitivity and value to the Group in accordance with the Group Information Classification Policy. The level of security protection to be provided to information throughout its lifecycle will depend directly on its classification. For details of the classification, please refer to 4.6.1.2 above.

8 Access Control Management

8.1 Access to information must be protected via access controls to ensure that it will not be improperly disclosed, modified, deleted, or rendered unavailable.

8.2 Information owners are responsible for determining who can access the information they own. Access rights shall be granted to individuals on an as-needed and least-privilege basis.

8.3 Privileged access gives a user the ability to perform any task on IT facilities which is necessary for the provisioning and administration of the facilities. However, to ensure the integrity and availability of IT facilities, privileged access is restricted by default. Any request for privileged access must be authorised by a department head or above of the IT Division and, if granted, it should only be used for the approved duration and all activities performed must be logged for auditing and future reference.

8.4 Process has been implemented to conduct periodic review of user access and privileges to verify that only legitimate users have access to information. The access rights will be revoked promptly once an individual is discharged from responsibilities that require the access need.

9 Information Privacy

9.1 The Group is committed to respecting and safeguarding the privacy of individual's personal data. Information containing personal data is being managed and protected in accordance with the Group Personal Privacy Policy.

10 IT Asset Management

10.1 In the context of this Policy, an IT asset is any device or service owned or managed by the Group such as server, storage system, network device, database, and application that connects to or used by the Group in its business operations. IT asset management is key to prudent security and management practices and covers all issue-specific information security policies, guidelines, procedures, and standard requirements.

10.2 IT assets are susceptible to attack. Therefore, the principle of security by design and security by default must be observed throughout the acquisition or development lifecycle. The Group has published guidelines to help individual business units

understand the fundamental data and system security requirements that must be met by IT assets provided by third parties. Besides, IT assets, being important resources, shall be maintained and supported systematically during their lifetime.

11 Network Security

11.1 Network infrastructure provides essential connectivity between internal and external systems. In order to provide mitigation against malicious activities, secure boundaries and connections must be established and managed in line with the latest security practices of the Group.

11.2 The Group's network architecture must commensurate with current and future business requirements and emerging security threats. Appropriate perimeter security technologies must be implemented to enable users throughout the Group to access untrusted networks (e.g. the Internet) from within while ensuring the internal networks of the Group remain secure.

12 Mobile Device Security

12.1 The Group embraces the use of mobile devices for business purpose as it offers agile and flexible work arrangements to the users. To minimise the risk while maximising the benefits of enabling its workforce with mobile devices, the Group has:

12.1.1 Implemented a mobile device onboarding process where mobile devices that can be used to access the Group's internal networks and information will be managed by appropriate mobile device management software and protected by security protection facilities.

12.1.2 Devised a Mobile Device Policy which sets out the rules and guidelines for the proper use, management, and security of mobile devices that are used to access information and IT assets for legitimate business purpose.

13 End-User Device Protection

13.1 End-user devices ("endpoint devices"), primarily desktop and laptop PCs, are the main gateways to IT facilities and information. An endpoint protection platform is a vital part of the Group's information security management as it represents the first line of defence in securing the internal networks.

13.2 The Group has implemented appropriate endpoint security facilities to provide comprehensive protection to endpoint devices from sophisticated malware and evolving cyber security threats. Besides, users are required to fully comply with the

standards set out in the Group Personal Computer Security Policy.

14 Remote Access

14.1 Remote access is defined as getting access to IT facilities and information assets through connection to the Group's internal networks from any device (laptop, mobile phone, or tablet) over untrusted networks, regardless of the location initiating the connection. Eligibility of employees or contractors for the remote access will be determined by the responsible business unit head.

14.2 Remote access will be strictly controlled with encryption and two-factor authentication. Authorised users must comply with the Group Remote Access Policy and take reasonable precautions to safeguard the Group's information and networks while using remote access.

15 Application Security

15.1 Security is a vital consideration during all stages of the application development lifecycle, particularly when it is developed to manage critical information and resources.

15.2 The Group is committed to taking a security-by-design and security-by-default approach to application design and development where security capabilities are incorporated into the application from the inception and throughout different stages of the development lifecycle with an objective to prevent security vulnerabilities against threats after application rollout.

16 Security Logging and Monitoring

16.1 The timely detection of information security incidents relies on continuous monitoring and comprehensive analysis of security logs generated by a myriad of security devices such as firewalls, intrusion detection systems, and email filtering appliances installed within the Group's DMZ (Demilitarised zone) and internal networks.

16.2 The Group has engaged an external security operations centre for round-the-clock proactive monitoring, security log analysis, and real-time correlation of security events within and around the Group's internal networks for early detection of and response to suspicious activities and security incidents.

17 Security Incident Management

17.1 The Group has implemented appropriate measures and facilities to detect security

incident. An incident handling process has also been established to ensure a quick, effective, and orderly response to incident with an objective to contain and limit its damage.

17.2 Post-incident review will be conducted to determine whether there is any underlying security issue that needs to be addressed through implementation of new or revised security controls.

18 Vulnerability Management

18.1 All IT facilities are susceptible to vulnerability and under constant threat from malicious exploitation that may lead to the compromise of confidentiality, integrity, and availability of information.

18.2 Vulnerabilities are addressed by applying vendor-supplied security patches. The Group Security Patch Management Policy is meant to ensure that IT facilities are updated accurately and timely with security patches for known vulnerabilities to protect the security of IT and information assets.

18.3 Alternatively, compensating controls can be used to address identified vulnerabilities if there is a true technical limitation (e.g. zero-day vulnerability) or business need prevents vulnerabilities from being corrected.

19 Change Management

19.1 The Group Change Management Guidelines for IT defines a standardised process to ensure that changes to IT facilities are managed properly, and that changes are recorded, evaluated, authorised, prioritised, implemented, and deployed in a systematic, secure, and controlled manner. The key objectives of the change management process are to (a) nurture a mindset of continuous improvement through regular review and learning, (b) review and prioritise changes according to business needs, (c) evaluate risk impact of changes and implement necessary mitigation measures as appropriate, (d) establish accountability and responsibility for changes throughout their lifecycle, (e) prevent unauthorised changes to IT facilities, and (f) minimise disruptions due to unplanned or emergency changes.

20 Disaster Recovery Planning

20.1 The Group has formulated disaster recovery plans (DRPs), implemented information backup operations and developed IT service recovery capabilities to ascertain that individual critical IT facilities and information assets can be recovered in case of disaster in a manner that aligns with business operational needs and priorities.

21 Third Party Risk Management

21.1 Engagement of contractors shall be enforced with appropriate information security controls with respect to the nature of works to be performed by the contractors. Specifically, security risks of the Group incurred by sharing proprietary and sensitive information with third-party vendors and suppliers must be operationally and contractually controlled.

21.2 To mitigate supply-chain related information security risks, the Group has established guidelines to assist individual business units to establish relevant information security controls for contracts of different nature and risk profiles. The guidelines also facilitate business units to conduct assessment to gauge and gain insight into the security posture of their contractors.

22 Information Security Awareness Education

22.1 Users must not be given access to information and IT facilities unless they have read and understood this Policy as well as various issue-specific security policies, standards, guidelines, and procedures. Individual business unit heads shall devise appropriate measures to demonstrate full compliance with this requirement.

22.2 Business unit heads shall make sure that their employees are aware of the security risks associated with their activities and have enough training and technical skills to be able to securely use the Group's IT facilities and IT assets to which they have been granted access.

22.3 IT shall provide refresher courses and other materials to regularly remind users of their obligations and responsibilities pertinent to information security.

22.4 IT shall conduct regular information security drills, analogous to fire drills, to ascertain preparedness and alertness of users, in addition to usual training and awareness activities.

23 Violation of Policy

23.1 All users are responsible for ensuring that no actual or potential security breaches occur due to their actions. Violation of this Policy will be treated by the Group as a serious disciplinary matter which may lead to disciplinary action including termination of employment.

23.2 Non-compliance by third parties will be handled in accordance with terms and

conditions set forth in the relevant contracts between the Group and the third parties.

24 Communication and Enquiries

24.1 Any enquiries or improvement suggestions regarding this Policy or any of the issue-specific security policies, standards, guidelines, or procedures should be addressed to the General Manager (Information Technology).

25 Policy Review

25.1 This Policy must be reviewed annually or more frequently if appropriate to ensure that all policy provisions remain fit for purpose.