# Information Security Policy

## A5 Organizational Controls

5.1 Policies for Information Security

5.1.1 Information Security Policy Document

1) The organization shall establish a written Information Security Management System (ISMS) policy to ensure confidence and safety in the use of information technology systems. This policy must be formally approved by the highest level of management prior to implementation.
2) The ISMS policy must be disseminated to relevant external parties and stakeholders within its scope to ensure awareness and compliance.

5.1.2 Review of the Information Security Policy

The ISMS policy must be reviewed, assessed, and updated at least annually, or whenever significant changes occur, whether internally or externally to the organization.

5.2 Information Security Roles and Responsibilities

5.2.1 Clear assignment of duties and responsibilities for personnel involved in information security operations must be established.

5.2.2 Executive management shall appoint a core team or working group, along with the necessary resources, to oversee and manage information security activities.

5.3 Segregation of Duties

Duties and responsibilities must be clearly defined and separated to minimize the risk of misuse of authority—either intentional or unintentional—that could cause harm to the organization.

5.4 Management Responsibilities

All employees and contractors must adhere to the organization's information security policies and practices. Management must:

5.4.1 Direct and support personnel to ensure the effectiveness of the Information Security Management System (ISMS).

5.4.2 Define strategic directions and review the ISMS to maintain information security across all processes.

5.4.3 Provide adequate resources for the effective implementation of the ISMS.

5.4.4 Communicate the importance of achieving effective information security and align operations with ISMS requirements.

5.4.5 Promote continual improvement of the ISMS.

5.5 Contact with Authorities – ISMS Contact List

5.5.1 A list of internal contacts responsible during emergencies must be established.

5.5.2 A list of external contacts for coordination during emergencies must also be established.

5.6 Contact with Special Interest Groups – ISMS Contact with Interest Groups

5.6.1 The organization must maintain an updated list of relevant interest groups in the field of information security for knowledge sharing and collaboration.

5.6.2 Contact details for other relevant agencies—such as the Royal Thai Police, internet service providers, and the Thai Computer Emergency Response Team (ThaiCERT)—must be maintained and regularly updated for coordination in case of security incidents or emergencies.

5.7 Threat Intelligence

The organization shall collect and analyze threat intelligence related to information security threats. This includes internal and external sources detailing threat vectors, techniques, technologies used by attackers, and emerging trends. The information shall be reviewed quarterly to ensure proactive risk mitigation and relevance to the evolving threat landscape.

5.8 Information Security in Project Management

5.8.1 Security requirements, including access control and data handling procedures, must be defined for all projects to ensure information security throughout project execution.

5.8.2 Projects involving third-party vendors or internal development must comply with IT project management procedures to ensure security and mitigate potential risks, including the use of outsourced service providers.

5.9 Inventory of Information and Other Associated Assets

5.9.1 Asset Inventory

1) A comprehensive asset inventory must be maintained, regularly reviewed, and updated at least annually or when significant changes occur.

2) The inventory must include assets such as hardware, software, AI models, datasets, information, networks, personnel, and services. Asset ownership and custodianship must be clearly assigned.

5.10 Acceptable Use of Information and Associated Assets

5.10.1 Clear procedures must be established for managing and storing information assets to prevent information leakage or misuse.

1. Users shall not leave or dispose of important information assets such as documents or storage media in unsecured locations, public areas, or places that are easily visible.
2. Handling of Assets
   (1) Confidential information must not be disclosed to unauthorized persons unless required for operational purposes.
   (2) Employees must be aware of their responsibility to protect the data stored on their workstations.
   (3) In shared workstation environments, confidential data must be protected using encryption or other appropriate operating system or IT security mechanisms.
   (4) Confidential documents and media containing sensitive data should be stored in lockable cabinets when not in use, especially outside of working hours or when left unattended.
   (5) Confidential data must be promptly removed from processing devices such as printers and copiers.
   (6) Employees must not disclose confidential information to external parties unless bound by a non-disclosure agreement.
   (7) Portable storage media and devices (e.g., USB drives) containing confidential data must be handled and used with care.

5.11 Return of Assets

Employees of KCG Corporation Public Company Limited who are exiting employment must return all company assets related to IT systems, including ID badges, access cards, keys, computers, peripherals, manuals, and documentation to their supervisors or designated officers before their last working day, in accordance with records maintained in the company's system.

5.12 Classification of Information and Information Assets

The classification of information must include the determination of sensitivity levels, criticality, and legal requirements for both physical (hardcopy) and electronic (softcopy) formats under the organization's responsibility. This ensures appropriate protection measures are implemented to secure information assets.

5.13 Labeling of Information

5.13.1 There must be established methods for labeling and managing tags for documents and related information assets.

5.13.2 Hardcopy documents must display labels indicating their confidentiality level. For softcopies, labels indicating importance and legal requirements should be embedded in the content. Departments shall determine the appropriateness of such labeling and may waive labeling requirements if justified.

5.14 Information Transfer

5.14.1 Information Transfer Policies and Procedures

All transmission of confidential data or electronic files between internal and external entities must be secured using encryption (cryptographic controls).

5.14.2 Agreements on Information Transfer

Formal agreements must be in place to govern the exchange of information or electronic files between the company and external parties. These must include signed confidentiality or non-disclosure agreements.

5.14.3 Electronic Messaging Security

Appropriate security measures must be implemented to safeguard electronic messages, including secure transmission over networks and access controls to protect sensitive data.

5.15 Access Control

5.15.1 Business Requirements for Access Control

1. Access Control Policy

(1) Information and IT system access must be controlled and limited to authorized users only.

(2) Access rights must be assigned based on job responsibilities and reviewed regularly to ensure appropriateness.

(3) Only system administrators are permitted to modify or update access rights.

(4) All access activities and changes in permissions, whether by authorized or unauthorized users, must be logged to support future investigations.

(5) Access to data and IT systems must be granted only upon proper authorization and must be limited to job-related functions. Information security and confidentiality are integral to IT policies and procedures, including account permissions, login credential management, access boundaries, data backup, and data recovery processes.

5.15.2 Access to Network and Network Services

1) Network administrators shall grant access rights to network systems and services strictly based on operational necessity.
2) Access to network and network services must be controlled, particularly to maintain the security of information and IT systems, including but not limited to:
   (1) Utilization of secure protocols for network administration, such as Secure Socket Layer (SSL), Simple Network Management Protocol (SNMP), and Web Certificates.
   (2) Restrictions on network usage that may impact bandwidth, such as the transfer of large files, online music streaming, video streaming, or online gaming during business hours.
3) The network must be properly designed and configured to ensure the security of information and IT systems. For instance:
   (1) All network-connected devices must be securely configured and monitored for network-related activities. Cabling systems must meet industry standards and be installed by qualified, approved personnel.
   (2) Network devices such as routers, firewalls, switches, and wireless access points must be configured according to their respective security requirements or manufacturer recommendations (e.g., SANS Institute or National Security Agency - NSA).

5.16 Identity Management

To ensure the unique identification of individuals and systems accessing information and related organizational assets, and to allow appropriate access provisioning.

The organization should establish processes to support identity data changes, which may include verification using trusted documentation.

When utilizing third-party or externally issued identities (e.g., social media credentials), the organization should ensure the identity data is trustworthy, and any related risks are acknowledged and adequately addressed. This may include applying controls related to third-party access and authentication data.

5.17 Authentication Information

5.17.1 Management of Secret Authentication Information of Users

1) Account administrators must maintain the confidentiality of user passwords.
   (1) Passwords must be at least 8 characters long and include a mix of uppercase letters, lowercase letters, numbers, and special characters (e.g., ! @ # $ % ^ & * ()).
   (2) Users must not reuse the last 4 passwords.
   (3) User accounts shall be locked after 5 failed login attempts.
2) Initial user passwords must be randomly generated by the account administrator.
3) Usernames and initial passwords must be delivered in sealed documents alongside assigned computer equipment.
4) Users shall be required to change their password immediately upon first login.

5) A system must be implemented to allow users to change their passwords, with mandatory password changes required annually.

5.17.2 Use of Secret Authentication Information

Usage and storage of secret authentication data must comply with company policies and procedures, including:

1) Username and password information must remain confidential and not be disclosed.
2) Avoid storing authentication data unless it can be secured appropriately.
3) Default credentials must be changed immediately upon initial system access.

5.17.3 Password Management System

A system must be in place to validate password strength and enforce periodic password changes. If a system cannot enforce this due to limitations, compensating controls must be implemented by the system administrator.

5.18 Access Rights

5.18.1 User Access Provisioning

1) Account administrators are responsible for assigning access rights to information and IT systems based on users' job responsibilities, as defined by the IT department's access control policies. Access rights must be reviewed at least annually or when changes occur.
2) Each user must be assigned a unique, non-overlapping account, which serves as their personal identification and authentication credential.
3) Where elevated privileges are required, approval must be obtained from the IT department, and such access must have defined usage periods and be revocable immediately upon role or employment changes.
4) In systems where account limitations necessitate shared user credentials, such credentials must be formally assigned by the IT department.
5) Users must acknowledge and accept the rights and responsibilities associated with using IT systems, and strictly adhere to all relevant policies.

5.18.2 Review of User Access Rights

1) Account administrators shall review user access rights at least annually or when there are changes in employment status, such as hiring, role changes, departmental transfers, retirement, or resignation.
2) A list of users with system access rights shall be compiled and submitted to department heads for review to ensure access aligns with job responsibilities.

5.18.3 Removal or Adjustment of Access Rights

1) Access rights must be immediately revoked upon employment termination, retirement, contract expiration, or when access is no longer required.
2) Access permissions must be adjusted in accordance with changes in job responsibilities, as notified by system owners. Users must be informed of any such changes.

5.19 Information Security in Supplier Relationships

5.19.1 Information Security Policy for Supplier Relationships

A formal agreement or contract outlining security obligations between the company and external suppliers must be established in writing.

5.20 Assessing Information Security within Supplier Agreements

5.20.1 Agreements with external suppliers must explicitly address security requirements related to access, processing, storage, communication, and IT infrastructure for company information. A comprehensive Service Level Agreement (SLA) must be established, covering service characteristics, security measures, and be subject to mutual acceptance and annual review.

5.20.2 Contracts must include non-disclosure clauses or a Non-Disclosure Agreement (NDA) to ensure the confidentiality of business and operational information shared during the engagement.

5.21 Managing Information Security in the ICT Supply Chain

5.21.1 Supplier agreements must address risk identification throughout the information supply chain.

5.21.2 Suppliers must be required to extend information security policies and practices to subcontractors (if any) involved in service delivery.

5.22 Supplier Service Delivery Management

5.22.1 Monitoring and Review of Supplier Services

1) Agreements must include audit rights to inspect the supplier's work environment and performance in accordance with the procurement contract.
2) Supplier performance must be regularly monitored and evaluated to ensure contractual compliance.
3) Performance results must be reviewed before contract renewal, renegotiation, or amendment.

5.22.2 Managing Changes to Supplier Services

1) Any changes in external service providers must be based on performance assessments and necessity.
2) Contract or agreement changes must be carefully evaluated and approved by authorized personnel, including risk assessment for potential business impacts during the transition.

5.23 Information Security for Using Cloud Services

The Company has implemented security control measures for cloud services to ensure enhanced protection of corporate data stored on cloud platforms. This encompasses procurement, usage, management, and termination of cloud services. Security measures have been established, including clear criteria for the selection of cloud service providers. Additionally, the Company has defined acceptable usage processes and established information security protocols for the termination of cloud services.

5.24 Management of Information Security Incidents and Improvements

5.24.1 Responsibilities and Procedures

Clearly defined responsibilities and procedures must be established to effectively respond to information security incidents. These procedures shall be timely, effective, and systematically implemented.

5.24.2 Reporting Information Security Events

Employees who observe any events or incidents related to information security must report them promptly to the relevant responsible parties to allow for timely investigation and remediation. Examples include computer viruses, data loss, and system failures.

5.24.3 Reporting Information Security Weaknesses

Controls must be implemented requiring employees, contractors, and service providers to record and report any suspected observations or weaknesses in information security within the systems or services.

5.25 Assessment of and Decision on Information Security Events

Controls must be in place to ensure that all information security-related events are assessed and appropriately classified. Decisions must be made accordingly when such events are categorized as information security incidents.

5.26 Response to Information Security Incidents

Controls must be in place to ensure that responses to information security incidents are conducted according to documented procedures.

5.27 Learning from Information Security Incidents

Knowledge gained from the analysis and resolution of information security incidents must be utilized to reduce the likelihood or impact of similar future incidents.

5.28 Collection of Evidence

The Company must establish and implement procedures for the identification, collection, acquisition, and preservation of information that may be used as evidence.

5.29 Information Security During Disruption

5.29.1 Information Security Continuity

A contingency plan must be developed to ensure preparedness for both electronic and physical emergency scenarios. The plan must include at a minimum:

1. Roles and responsibilities of all relevant personnel.
2. Procedures for recovery of IT systems.
3. Procedures for data backup and testing of backup recovery.
4. Contact channels with external service providers.

5.29.2 Implement Information Security Continuity

A written emergency response plan must be maintained and regularly updated. The plan must be tested at least once per year to ensure its effectiveness and relevance.

5.29.3 Verify, Review, and Evaluate Information Security Continuity

1. A defined schedule and timeframe for emergency plan testing must be established.
2. Simulated events must be clearly detailed, including test objectives, scope of affected systems or processes, and step-by-step test procedures.

5.30 Necessary resources, responsible coordinators, locations, equipment, and budget allocations must be identified. A clear roadmap for reviewing and updating the plan must be outlined to ensure ongoing relevance. ICT readiness for business continuity must be planned, implemented, maintained, and tested according to business continuity objectives and ICT continuity requirements. The Company must ensure ICT systems and infrastructure are adequately prepared for potential disruptions to maintain the availability of essential information and assets.

Business impact analysis, continuity strategies, and continuity plans must be documented, tested annually, and formally reviewed by executive management.

5.31 Legal, Statutory, Regulatory, and Contractual Requirements

5.31.1 Identification of Applicable Legislation and Contractual Requirements

All users must acknowledge, understand, and strictly comply with applicable policies, laws, regulations, and contractual obligations related to the use of IT systems. The Information Technology Director serves on the Compliance Committee, which meets regularly. The minimum applicable laws and regulations include:

1. Computer-Related Crime Act
2. Copyright Act
3. Personal Data Protection Act (PDPA)
4. Royal Decree on Secure Methods of Electronic Transactions
5. Company's Information Security Policy and Practices (KCG Corporation Public Company Limited)

5.31.2 Regulation of Cryptographic Controls

Cryptographic controls must comply with relevant agreements, legal requirements, and applicable regulations.

5.32 Intellectual Property Rights

5.32.1 Users must comply with copyright regulations when using intellectual property provided by KCG Corporation Public Company Limited.

5.32.2 The use of software must be managed and controlled in accordance with licensing agreements.

5.32.3 Users are strictly prohibited from using, reproducing, or distributing copyrighted materials—including images, music, articles, books, or documents—or installing pirated software on any company-owned devices.

5.33 Protection of Records

Records must be retained as evidence of compliance with regulatory and legal requirements. The retention period must be based on the importance of the data.

5.34 Privacy and Protection of Personally Identifiable Information (PII)

The Company is committed to protecting personal data in accordance with applicable legal and contractual requirements.

5.35 Independent Review of Information Security

Information security management practices, objectives, policies, and procedures must be independently reviewed for accuracy and currency at least annually or when significant changes occur.

5.36 Compliance with Policies, Rules, and Security Standards for Information Security

5.36.1 Compliance with Security Policy and Standards

1. Full system audits must be conducted per the Company's information security policies and within defined intervals.
2. All security policies, procedures, and related documentation must be reviewed and updated according to scheduled intervals or upon changes.

5.36.2 Technical Compliance Review

Technical configurations of operational systems must be reviewed regularly to ensure sufficient information security. This includes:

- Assessing vulnerability to system breaches
- Ensuring secure parameter configurations
- Conducting vulnerability scanning
- Performing penetration testing to identify system weaknesses

5.37 Document Operating Procedures

5.37.1 Appropriate operational procedures must be documented for each IT system under the user's responsibility and communicated to relevant personnel.

Operational manuals and procedures must be updated upon changes in processes or responsibilities. All related documents must be reviewed at least annually and secured against unauthorized access.

**A6 Personnel Control Measures (People Control)**

6.1 Recruitment and Screening

6.1.1 The Human Resources Department shall conduct background checks on all prospective personnel. Individuals applying for a position are required to submit personal documentation, such as a copy of their national identification card and household registration, for verification. A criminal background check must also be conducted through the Royal Thai Police.

6.1.2 The Human Resources Department shall verify the qualifications of all candidates prior to their appointment as executives, temporary staff, or interns. Candidates must not have any prior record of unauthorized access, modification, destruction, or theft of information within any organization's information technology systems.

6.1.3 All personnel must sign a Non-Disclosure Agreement (NDA) before commencing employment with KCG Corporation Public Company Limited.

6.1.4 External service providers performing activities within the company must sign a Non-Disclosure Agreement (NDA) or an agreement relating to information security (Security in Third Party Agreements) prior to engaging in any operational activities within KCG Corporation Public Company Limited.

6.2 Terms and Conditions of Employment

The Human Resources Department must ensure that employment contracts clearly outline job responsibilities, including general duties based on the position and specific obligations concerning information security.

6.2.1 To ensure proper and up-to-date management of login credentials or user IDs, the Human Resources Department must promptly notify the Information Technology Department of the following situations:

1. New employment
2. Resignation, termination of employment, or death of an employee
3. Departmental transfers
4. Suspension, disciplinary action, or temporary removal from duties

6.3 Information Security Awareness, Education, and Training

6.3.1 All employees must receive appropriate training aligned with their roles and responsibilities to promote awareness and understanding of information security.

6.3.2 Employees must be educated on information security practices, including awareness and procedures necessary to ensure system security. This includes communication regarding security policies and any updates or changes thereto.

6.3.3 All new employees must undergo training on the company's information security policies.

6.3.4 An annual training plan must be established to provide employees with information security education at least once per year.

6.4 Disciplinary Process

The highest-level management is responsible for establishing disciplinary measures for violations of company policies, rules, and/or procedures. If the violation constitutes a breach of law, penalties shall be imposed in accordance with the relevant legal provisions.

6.5 Responsibilities After Termination or Change of Employment

6.5.1 Termination or Change of Employment Responsibilities

1) Employees or contractors must be informed of and comply with contractual obligations upon termination or change of responsibilities.
2) The Human Resources Department is responsible for managing any appointments, transfers, dismissals, or position changes related to company responsibilities.
3) The Human Resources Department must notify the Information Technology Department of changes in employment status to revoke or modify access rights. The IT Department shall proceed as follows:
   (1) Microsoft Active Directory accounts / Access Card Systems: Employee access rights shall be revoked by midnight on the employee's final day of employment.
   (2) Urgent Access Termination: Immediate revocation will occur upon notification.

6.6 Confidentiality and Non-Disclosure Agreements

All employees and external service providers must sign a written confidentiality or Non-Disclosure Agreement (NDA) to safeguard sensitive information. These agreements shall be regularly reviewed and documented appropriately.

6.7 Teleworking

6.7.1 Employees and external service providers who require remote access to the company's IT systems must be clearly identified, and the devices used for access must be controlled or managed by the company.

6.7.2 Remote access to the company's IT systems must only be conducted via the company-specified Virtual Private Network (VPN).

6.7.3 Personal devices used for remote access must have up-to-date antivirus protection and a firewall in accordance with company requirements.

6.7.4 Procedures must be established for the approval and revocation of remote working arrangements.

6.8 Information Security Event Reporting

6.8.1 Employees who encounter any events or incidents that may affect information security—such as computer viruses, data loss, or system failures—must promptly report them to the relevant personnel for timely investigation and resolution.

6.8.2 Employees, contractors, and service providers must record and report any observed or suspected vulnerabilities in the company's IT systems or services in accordance with established procedures for reporting information security weaknesses.

**A7 Physical Controls**

Physical and Environmental Security of the Company

7.1 Secure Areas

7.1.1 Physical Security Perimeter

1. Areas requiring security controls (secure areas) must be clearly defined, such as the network room.
2. Physical measures must be in place to prevent unauthorized individuals from accessing these secure areas.

7.2 Controlled Physical Entry

7.2.1 Access control mechanisms such as fingerprint scanners or door locks must be installed.

7.2.2 CCTV systems must be installed to provide comprehensive coverage of controlled areas.

7.2.3 Authorized personnel lists for access to controlled areas must be maintained and reviewed at least once per year.

7.2.4 Delivery and Loading Areas

1. Designated delivery/loading areas must be established and, if possible, separated from operational areas to prevent unauthorized access.
2. All materials and goods must be inspected before being brought into controlled areas.

7.3 Securing Offices, Rooms, and Facilities

Offices, workspaces, and facilities must be organized and managed in accordance with safety and security standards applicable to office environments.

7.4 Physical Security Monitoring

The company must implement controls and monitoring mechanisms for sensitive areas, ensuring that only authorized personnel have access. This includes the office premises and network room. Clear procedures must be established for area inspections, personnel responsibilities, and communication channels for reporting physical security incidents.

7.5 Protection Against Physical and Environmental Threats

Appropriate safeguards must be in place against physical and environmental threats including fire, civil unrest, or natural/man-made disasters. Physical security systems must be tested at least once per year.

7.6 Working in Secure Areas

7.6.1 External visitors or service providers must receive prior authorization before entering controlled areas.

7.6.2 All entries to controlled areas must be logged, including the purpose of access.

7.6.3 External personnel are prohibited from bringing weapons, prohibited items, or flammable materials, except for standard office equipment.

7.6.4 Photography, smoking, food, and beverages are strictly prohibited within controlled areas.

7.7 Clear Desk and Clear Screen Policy

7.7.1 Confidential or sensitive information in physical or electronic form must be securely stored when not in use.

7.7.2 Workstations must be locked using passwords or other authentication mechanisms when not in use.

7.7.3 Confidential documents must not be left unattended on desks, and critical data should not be visible on screens when unattended.

7.8 Equipment Siting and Protection

7.8.1 Equipment Siting and Protection

1. Equipment must be located in secure areas and protected from damage, supported by utilities such as signal cables, air conditioning, and UPS systems to ensure business continuity.
2. IT equipment must be positioned to prevent unauthorized individuals from viewing sensitive information.

7.8 Security of Off-Premises Information Assets

7.9.1 Authorization must be obtained before using IT equipment outside of the company premises.

7.9.2 Information assets must not be left unattended.

7.9.3 Personnel must treat company-owned IT equipment and data with the same level of care as personal property.

7.10 Storage Media

7.10.1 Management of Removable Media

1. Procedures for managing removable storage media must align with the company's data classification policy.
2. Storage media containing data must be protected from unauthorized access.

7.10.2 Disposal of Media

1. Destruction of documents or media must be approved by the data owner and appropriately recorded.
2. Destruction of data must be performed according to formal procedures to prevent unauthorized deletion.

7.10.3 Physical Media Transfer

No employee shall remove company assets or devices from company premises without authorization from department heads or designated authorities.

7.10.4 Removal of Assets

1. Unauthorized removal of IT assets for external use is prohibited.

2. Asset movement and return must be recorded for loss prevention.

7.11 Supporting Utilities

7.11.1 The company must provide adequate utility support systems such as electricity, temperature control, air conditioning, and backup power systems.

7.11.2 Mechanisms must be in place to prevent failure of utility systems to ensure the continuity of IT operations and business processes.

7.12 Cabling Security

Power and communication cables must be protected from unauthorized access or damage to ensure uninterrupted service and prevent tampering.

7.12.1 Cables entering the building must be routed through ceiling or underground conduits to prevent unauthorized access.

7.12.2 Network cables must not pass through areas accessible to external parties, to prevent signal interception.

7.12.3 Cable cabinets or distribution points must be locked and access limited to authorized personnel only.

7.12.4 Cables must be enclosed in conduits to prevent signal tapping, damage by animals, or cutting.

7.12.5 Power and communication cables must be routed separately to avoid signal interference.

7.12.6 Cables and equipment must be clearly labeled for ease of identification and troubleshooting.

7.12.7 Cable layouts must be documented and updated regularly.

7.12.8 Rooms housing communication cables must be locked to restrict unauthorized access.

7.13 Equipment Maintenance

All equipment must be regularly inspected and maintained. Maintenance must be conducted at least once per year.

7.14 Secure Disposal or Reuse of Equipment

7.14.1 Prior to disposal or redistribution, equipment containing sensitive information (e.g., hardware, software) must be thoroughly inspected to prevent data leakage.

7.14.2 All data on equipment must be erased before reuse.

**A8. Technological Control Measures**

8.1 Use of User Endpoint Devices

8.1.1 Policy on the Use of Mobile Computing Devices

1. Employees of KCG Corporation Public Company Limited should be aware of the need to protect and safeguard mobile communication devices both physically and in terms of the sensitive data stored therein. Physical protection includes securing devices to desks or storing them in lockable cabinets. To protect sensitive data, access by unauthorized individuals must be prevented through encryption. Additionally, critical data stored on such devices should be backed up regularly.
2. Employees must obtain prior approval before connecting their personal mobile communication devices (e.g., laptop computers, notebooks, tablets, smartphones, or other mobile devices) to the company's network. Furthermore, employees must be cautious when connecting company-owned mobile devices to external networks.

8.1.2 Protection of Unattended User Equipment

1. Users must prevent unauthorized individuals from accessing unattended IT equipment, computers, and network systems.

2. Users must log off from IT systems immediately upon completing their tasks and shut down computers at the end of each workday.
3. System administrators must configure computers to automatically activate a password-protected screen saver or lock screen after 10 minutes of inactivity.

8.2 Management of Privileged Access Rights

8.2.1 User accounts with elevated access privileges (e.g., Root or Administrator accounts) shall be assigned only to personnel with a demonstrated need, and access shall be time-bound to match the scope of the assigned duties.

8.2.2 In cases where elevated access rights must be granted to internal or external parties, the following strict controls must be applied:

1. Approval must be obtained from the system owner.
2. Access must be limited to essential usage only.
3. Access must be time-bound and promptly revoked after the access period ends.
4. Passwords must be changed immediately after the completion of access.

8.3 Information Access Restrictions

8.3.1 Access to information within IT systems must be controlled through permissions defining the ability to read, write, or delete data. Access rights must be granted only to users or groups requiring them, and information must be limited to that which is necessary for their roles.

8.3.2 Privileged accounts such as Root or Administrator must be assigned based on necessity and with limited access durations.

8.3.3 External parties must obtain authorization prior to accessing the company's IT systems.

8.4 Access Control for Source Code

8.4.1 IT system developers must store source code and software libraries in secure, protected locations.

8.4.2 Source code under development or testing must be stored separately from production source code.

8.5 Secure Authentication Procedures

Secure log-on features must be implemented for any newly approved systems, including:

8.5.1 Withholding system names or details until login is successful.

8.5.2 Disabling or hiding help functions during the login process.

8.5.3 Logging both successful and unsuccessful login attempts for audit purposes.

8.5.4 Concealing password inputs on screen during entry.

8.6 Capacity Management of IT Resources

8.6.1 Resource utilization and capacity of IT assets must be regularly monitored and analyzed to ensure proper planning for future operational needs.

8.6.2 Capacity planning must be conducted at least once a year, taking into account projected needs (e.g., faster CPUs, increased storage), current resource usage, and emerging technological developments.

8.7 Protection from Malicious Software (Malware)

8.7.1 Control Measures Against Malware

1. Endpoint devices, including portable computers, must be equipped with up-to-date antivirus software.

2. Server systems responsible for malware protection must also be kept current with the latest updates.

8.8 Management of Technical Vulnerabilities

8.8.1 Management of Technical Vulnerabilities

1. Information regarding vulnerabilities in current systems must be monitored, with risks assessed and mitigation measures implemented accordingly.
2. Security-related software must be regularly updated to address known vulnerabilities. The list of permissible software installed on user endpoints must also be strictly controlled.

8.8.2 Technical Compliance Reviews

Regular technical reviews must be conducted to ensure IT systems remain sufficiently secure. These reviews include vulnerability scanning, configuration assessments, and penetration testing to identify weaknesses.

8.9 Configuration Management

The company must manage the entire lifecycle of security configurations for its IT systems. This includes establishing configuration policies, implementation procedures, monitoring, and periodic reviews to ensure proper authorization of changes. All configuration changes must be reviewed at least annually or when changes occur.

8.10 Information Deletion Control

Information no longer needed must be deleted from IT systems and storage media to prevent unnecessary disclosure, in compliance with the Personal Data Protection Act (PDPA).

When using cloud services, the company must verify that deletion methods provided by the vendor are acceptable. Automated deletion processes aligned with internal policies should be used where applicable, with auditable logs maintained.

Sensitive data must be protected before devices are returned to vendors—e.g., by removing hard drives or memory storage.

8.11 Data Marking

8.11.1 Data masking should be implemented based on internal access control policies, applicable legal requirements, and contractual obligations, especially for personally identifiable and sensitive information.

8.11.2 Where there is concern regarding the protection of sensitive personal data, the company should implement technical measures such as redaction, pseudonymization, or anonymization.

8.11.3 When applying pseudonymization or anonymization, the adequacy and effectiveness of the techniques must be assessed. All attributes of sensitive data must be evaluated to ensure true de-identification, considering the risk of re-identification through indirect means.

8.12 Data Leakage Prevention Control

Preventive measures must be in place to avoid unauthorized disclosure of sensitive information. In the event of a data leakage incident, timely detection must be possible. These measures include classification of confidential information, risk assessments, vulnerability identification, and data protection controls.

8.13 Information Backup

8.13.1 Backup Procedures

1. Backup frequency must align with the criticality of the data and the risk tolerance defined by the data owner.
2. Backup systems and devices must be maintained to ensure operational readiness.
3. Physical access to backup storage locations must be controlled in accordance with the importance of the associated IT systems.
4. All systems must have documented backup and restoration procedures, with regular testing to verify backup integrity and restorability.
5. Data transfers between operational systems and backup storage facilities must be audited at least once a year.

8.14 Redundancy of Information Processing Facilities

Availability of Information Processing Facilities

8.14.1 Information processing facilities must be adequately provisioned with redundancy to meet the required levels of availability.

8.14.2 Regular testing of backup operational systems must be conducted to ensure they are capable of replacing primary systems when necessary.

8.15 Logging and Monitoring

8.15.1 Event Logging

1. Computer systems and network infrastructure must maintain activity logs that record user actions and security-related events. These logs are essential for future investigations, access control auditing, and must be analyzed regularly to identify and correct anomalies effectively.
2. IT administrators must implement procedures for ongoing monitoring of information systems usage and conduct periodic evaluations of these monitoring activities.
3. IT administrators must retain computer traffic data for a period not less than 90 days, in compliance with applicable regulations.

8.15.2 Protection of Log Information

Controls must be in place to protect log data from unauthorized alterations or modifications to preserve the integrity and authenticity of recorded information.

8.15.3 Administrator and Operator Logs

All administrative activities and operations performed by IT administrators or related personnel must be recorded, including actions involving computing devices and network systems.

8.16 Monitoring Activities

8.16.1 The company shall establish a review process to evaluate the adequacy and effectiveness of internal control systems within each functional unit. The objective is to ensure operational efficiency, effectiveness, and value-for-money, with continuous improvement aligned to evolving circumstances.

8.16.2 The company should monitor network systems and applications to identify abnormal behaviors and respond appropriately to potential information security incidents. This includes early detection of anomalies and response to security breaches.

8.16.3 Monitoring should be defined in terms of scope and depth based on business requirements and information security needs, in alignment with relevant laws and regulations. Monitoring records should be retained in accordance with defined retention policies.

8.17 Clock Synchronization

Time synchronization must be achieved using a recognized time source, such as Network Time Protocol (NTP), in accordance with information security management standards. This ensures consistency of timestamp data across event logs from IT systems and network devices, thereby supporting accurate forensic analysis.

8.18 se of Privileged Utility Programs

8.18.1 The use of privileged utility programs, which may override established security controls, must be strictly controlled and monitored. Access and usage must be limited to authorized personnel and should include the following controls:

1. Authentication must be required prior to use.
2. Access must be restricted solely to authorized personnel.
3. All usage must be logged, including identification of the user and relevant access details.

8.19 installation of Software on Operational Systems

8.19.1 Installation of new software, libraries, or security patches on operational servers must be controlled. Software must be thoroughly tested prior to installation to ensure it does not disrupt current operations.

8.19.2 Restrictions on Software Installation

1. All software usage must comply with intellectual property rights and licensing agreements.
2. Software installations must adhere strictly to copyright requirements. Proof of license ownership must be documented, and periodic audits must verify compliance.

8.20 Network Security

8.20.1 Network Control

1. Network administrators must restrict access to IT systems connected to the network and enforce user authentication mechanisms.
2. Security testing must be conducted before connecting to external networks to prevent unauthorized access.
3. Unauthorized network services must not be enabled.
4. Physical and remote access to network devices must be limited to authorized network administrators only.
5. Temporary access for third parties must be authorized and controlled.
6. Access privileges for external parties must be revoked immediately after tasks are completed.
7. Unused ports on network devices must be disabled.
8. Only essential ports and services necessary for system operation should be enabled on servers.
9. Network equipment security patches must be updated regularly.
10. A current and accurate network diagram, outlining internal network boundaries, must be maintained.
11. Computer traffic logs must be maintained in compliance with applicable laws.

8.21 Security of Network Services

8.21.1 Users must only utilize network services as authorized by the network administrator.

8.21.2 Users must avoid activities that degrade network performance, such as uploading or downloading large files.

8.21.3 Connecting devices to the corporate network without prior authorization is strictly prohibited.

8.21.4 Network usage for unlawful activities is strictly prohibited.

8.21.5 Users must access the network using only their assigned credentials.

8.21.6 Unauthorized disclosure of personal or organizational data is strictly prohibited.

8.21.7 External parties must not connect any computer or device to the corporate network without prior, explicit approval.

8.21.8 Users must not install network-related hardware or software (e.g., routers, switches, hubs, wireless access points) without proper authorization.

8.22 Segregation in Network

8.22.1 Systems that provide IT services directly to users, such as intranet and email systems, must be operated on networks accessible to authorized users.

8.22.2 Backend systems, such as databases, directory services, DNS, and printer services, must operate on networks that are not directly accessible by end-users.

1. User-accessible networks must be logically separated from system-focused networks.
2. Wireless access for mobile and smart devices must be provided via dedicated network zones.
3. Network architecture must be designed based on service groupings and user roles, implementing internal and external zones to strengthen intrusion prevention controls. A comprehensive and up-to-date network diagram must define both internal and external network scopes and components.

8.23 Web Filtering

The Company implements automated control mechanisms to filter and restrict access to unsafe or high-risk websites. Users are not able to determine which websites are secure or malicious. The Information Technology Department is responsible for inspecting and defining the web filtering policy, which must be reviewed at least once annually or whenever changes occur.

8.24 Use of Cryptography

8.24.1 Policy on the Use of Cryptographic Controls

(1) In circumstances where information confidentiality must be safeguarded through encryption, personnel of KCG Corporation Public Company Limited are required to utilize cryptographic techniques or methods as defined in the Company's Information Security Management Standards.

(2) For the internal computer networks of KCG Corporation Public Company Limited, any measures to protect communication confidentiality via encryption must adhere to the techniques or procedures established in the Company's Information Security Management Standards.\

8.24.2 Key Management

Cryptographic keys used within the Company's internal computer networks must be strictly managed, including key generation, storage, rotation, and ownership, to ensure secure and controlled access.

8.25 Security in Development and Support Processes

8.25.1 Secure Development Policy

Criteria must be established for software development that comply with the Company's policies and standards. Security considerations must be integrated throughout all development phases. Developers should possess the competency to prevent vulnerabilities in the software and to remediate any discovered security flaws.

8.26 Application Security Requirements

8.26.1 Securing Application Services on Public Networks

Information transmitted over public networks related to information services must be protected against unauthorized disclosure or modification.

8.26.2 Protecting Application Services Transactions

Information associated with application service transactions must be safeguarded against incomplete transmission, misrouting, data tampering, unauthorized disclosure, or delay in delivery.

8.27 Security System Architecture and Engineering Principles

8.27.1 Secure System Engineering Principles

Security principles for system engineering must be documented, continuously improved, and applied to all system development activities.

8.28 Secure Coding

8.28.1 Secure coding practices must be established to ensure software is developed in a secure manner, minimizing information security vulnerabilities.

8.28.2 The Company shall establish company-wide processes for secure coding oversight, including setting minimum security baselines. This governance should also extend to third-party and open-source software components.

8.28.3 The Company should monitor real-world threats, current advisories, and software vulnerability disclosures to inform and adapt its secure coding practices through continuous learning and improvement.

8.28.4 Secure coding principles must apply to both newly developed and reused software components, across internal development efforts and products/services delivered to external parties. These principles must be considered during planning and initial requirement stages.

8.29 Security Testing in Development and Acceptance

8.29.1 System Security Testing

1) Security features of developed systems must be tested throughout the development process.
2) Developers must implement input validation controls.
3) Developers must implement processing validation controls to ensure accuracy and detect anomalies.
4) Developers must ensure data transmission is secure, accurate, and intact.

8.29.2 System Acceptance Testing

Test plans and acceptance criteria must be defined for both new and modified systems.

Acceptance criteria must be established for newly developed, procured systems or other information assets before they are put into operation. A test checklist must be completed and signed by both the testing personnel and the system provider.

8.30 Outsourced Development

Contracts with external developers must clearly define the scope, including intellectual property rights, system inspection procedures prior to deployment, quality assurance standards, and development boundaries.

8.31 Separation of Development, Testing, and Production Environments

8.31.1 Separation of Development, Testing, and Operational Environments

Development and production environments must be segregated, including computer systems and networks, to minimize the risk of unauthorized access or system modifications.

8.31.2 Secure Development Policy

Software development guidelines must be established and adhered to, ensuring that security is considered at every stage. Developers must have the capability to prevent and remediate vulnerabilities within their software.

8.32 Change Management

8.32.1 Change Management

1) Prior to making changes to IT systems, networks, software, or databases, administrators or external service providers must obtain formal written approval from the IT Department.
2) All changes performed by external providers must be supervised by IT administrators.
3) IT administrators must notify users prior to any system changes.
4) All changes must be evaluated for potential impacts before implementation to avoid operational disruptions.
5) Change records must be documented by IT administrators.
6) All changes, especially to critical systems, must undergo testing before deployment.
7) A fallback plan must be defined to address unexpected outcomes.
8) A post-change monitoring period must be established to assess any residual impact.

8.32.2 System Change Control Procedures

A structured change control process must be in place for live systems. This includes:

1) Change requests must originate from authorized personnel.
2) Requests must be approved by authorized parties.
3) Potential side effects of changes must be assessed and controlled.
4) All changes must be verified and accepted post-implementation.
5) All change request records must be maintained.

8.32.3 Technical Review of Applications After Operating Platform Changes

Following modifications to operating systems, developers must review and test applications to ensure continued functionality and security.

8.32.4 Restrictions on Changes to Software Packages

Changes to off-the-shelf software should be limited to what is necessary. All modifications must be tested and documented for reusability.

8.33 Test Information

8.33.1 Protection of Test Data

1) Real production data, especially personal or confidential information, must not be used in testing environments. If necessary, explicit consent from the data owner must be obtained, and adequate controls must be in place to prevent unauthorized duplication.
2) After testing is completed, real data must be removed from test environments, and its use must be documented, including the test purpose, dates, and responsible personnel.

8.34 Protection of Information Systems During Audit Testing

8.34.1 Information System Audit Controls

All IT audit activities must be pre-planned to ensure minimal disruption to systems and business operations during execution.

Announced on June 5, 2025

*-Nuttachai Veerakul-*

Mr. Nuttachai Veerakul

Chief Corporate Strategy Officer