Information Technology and Cybersecurity Policy

Siamgas and Petrochemicals Public Company Limited and its subsidiaries ("the Company") has established a computer network to facilitate employees in carrying out their duties for the Company. To ensure the appropriate and efficient use of the computer network, as well as to prevent potential issues arising from improper usage.

Chapter 1: Definitions

"the Company" refers to Siamgas and Petrochemicals Public Company Limited and its subsidiaries.

"Computer Network" refers the computer network of Siamgas and Petrochemicals Public Company Limited and its subsidiaries.

"Supervisor" refers to individuals with command authority as per the Company structure of Siamgas and Petrochemicals Public Company Limited and its subsidiaries.

"Employee" refers to employees and staff of Siamgas and Petrochemicals Public Company Limited and its subsidiaries, including individuals assigned by the Company to perform duties under contracts, agreements, or purchase orders.

"Data" refers to information that conveys facts, stories, or any type of content, regardless of whether that information is expressed directly or through any medium, and regardless of format, such as documents, files, reports, books, diagrams, maps, drawings, photographs, film, audiovisual recordings, computer records, or other retrievable formats.

"Network Administrator" refers to employees assigned by supervisors to manage and maintain the computer network system, including access to network software for managing the network database.

Chapter 2 : Roles and Responsibilities of the Information Technology and Cybersecurity Committee

The " Information Technology and Cybersecurity Committee" shall be appointed by the supervisor from among the Company's employees and shall be responsible for:

- Supervising and advising network administrators on compliance with this regulation
- Providing consultation to network administrators regarding these regulations
- Recommending policies and security measures to the supervisor
- Preparing reports on the enforcement of these regulations as appropriate
- Performing other duties specified under this regulation

- Executing tasks assigned by the supervisor

Chapter 3: Employee Responsibilities in Using the Computer Network

1. Employees may use the computer network under the provisions of these regulations. Any violation causing or potentially causing harm to the Company or others may result in disciplinary and legal action.
2. Employees shall use network resources efficiently, avoiding unnecessary large file downloads and high-traffic usage during working hours.
3. Employees must use polite and appropriate language in communications and follow proper etiquette when using the network. For example, they should avoid unnecessary mass email broadcasts to all network members and should use respectful wording in messages sent to others.
4. Employees must secure their network account credentials and must not allow others to use their accounts.
5. Employees must not use the computer network for:
    - Committing illegal acts or causing harm to others
    - Engaging in actions that violate public order or moral standards
    - Commercial purposes
    - Disclosing confidential information obtained while performing duties for the Company, whether such information belongs to the Company or third parties
    - Acts that infringe upon the intellectual property rights of the Company or others
    - Accessing others' information without permission from the rightful owner or authorized person
    - Transmitting or receiving data that causes or may cause damage to the Company, such as chain letters or data from external parties that may violate the law or infringe upon others' rights, and forwarding such data to employees or others
    - Obstructing the use of the Company's network or that of other employees, or rendering the network inoperative
    - Expressing personal opinions related to the Company's operations on websites in a manner that may cause misunderstanding or misrepresentation of facts
    - Any other actions that may conflict with the Company's interests or cause disputes or damage to the Company

6. For overall network security, employees must:
    - Not install computer programs that infringe on the intellectual property rights of others
    - Not install computer programs capable of monitoring network information unless authorized by a supervisor
    - Not install additional computer programs or hardware on the Company's devices that allow third parties to access the Company's devices or network
    - Shut down their personal workstation after daily use or after more than one hour of inactivity, unless the device functions as a server that must operate 24/7
    - Scan all data received from outside the organization using antivirus software provided by the organization, and if any virus is found, promptly remove it or delete the infected data
    - Delete unnecessary data from their workstation to conserve storage resources
    - Use encrypted software provided by the Company for external access to the Company's network
    - Cooperate with and facilitate supervisors, network administrators, or the Information and Network Security Committee in inspecting the security of personal workstations and the organization's computer network, and follow all recommendations and guidance from such authorities
    - Exercise care and caution in handling and preserving both personal workstations and the Company's network equipment, as would be expected from any responsible user
    - Not access network infrastructure locations without prior authorization
    - Return all company -owned IT assets (e.g., data and data copies, keys, ID cards, access passes) and request return of any personal data on the network within 7 days of termination of employment

Chapter 4: Password Policy

1. Users are responsible for protecting and maintaining the confidentiality of their account credentials (username and password). Each user must have their own individual username and must not share or disclose it or their password to others.
2. Users are accountable for any action taken under their account, regardless of whether they performed the action themselves.

3. Upon receiving their initial password, users must immediately change it to a new, secure password that is difficult to guess. All End Users are required to change their passwords every 90 days or whenever prompted by the system to do so. Users must change their password every 90 days or whenever prompted by the system.
4. Users must authenticate themselves before accessing any IT resources or equipment of the Company. In case of authentication issues, such as a locked password or technical problems, users must notify the system administrator immediately. Additionally:
   (1) Internet and intranet access must be authenticated and recorded to identify the user
   (2) Users must log out of their sessions whenever they are away from their workstation

Chapter 5: The User administration procedure

1. Network administrators must maintain and update the computer network system to ensure proper functionality at all times. They must also monitor employee usage to ensure compliance with these regulations. If any employee exhibits behavior that suggests a violation, the network administrator must promptly report it to the Information and Network Security Committee and the appropriate supervisors. In urgent situations to prevent potential damage, the network administrator has the authority to immediately suspend the employee's network access.
2. Network administrators shall provide opinions and observations to the Information and Network Security Committee and higher-level supervisors regarding improvements to network efficiency and management, or perform other network-related duties as assigned.
3. Network administrators are responsible for installing and maintaining equipment, software, automatic data encryption systems, or any other systems related to the computer network to ensure continuous operation.
4. Network administrators must not misuse their authority to access transmitted data without proper rights, and must not disclose any information obtained in the course of their duties that is considered confidential.
5. Upon leaving their position, network administrators must return all company owned items related to their duties such as data and data copies, keys, ID cards, and access passes immediately. The Information and Network Security Committee must conduct a thorough inspection of the returned items to ensure network and data security.

6. Any network administrator who violates these regulations and causes or may cause harm to the Company or any individual may be subject to disciplinary and/or legal action as deemed appropriate.

Chapter 6: Backup and Restoration

1. Create and store backup copies of IT data, organized by level of importance to the Company.
2. Implement accurate and systematic backup and restoration procedures for each operational system.
3. Establish an emergency preparedness plan that enables timely restoration of systems in the event of an incident.

Chapter 7: Review of User Authorization (ERP/SQL Server/Windows Server)

1. Prepare and maintain a list of user accounts and corresponding access rights, and designate responsible personnel to verify the information.
2. Conduct a review to ensure the accuracy and completeness of all user accounts and access rights. Submit the user list to the relevant departments for review and confirmation by the department head or their designated representative, and report the results to the Information Technology Department.
3. Perform an annual review of ERP user access rights at a minimum.

Chapter 8: Cybersecurity Protection

1. Conduct Vulnerability Assessments and Penetration Testing at least once a year to identify, assess, and remediate potential vulnerabilities and security risks within the Company's information systems.
2. Implement appropriate measures to prevent data leakage and unauthorized disclosure of information, including the deployment of firewalls, encryption of data both at rest and in transit, and the enforcement of access controls based on the principle of least privilege, ensuring that access to sensitive information is restricted to authorized personnel with a legitimate business need.
3. Cybersecurity Awareness Training to employees to enhance their knowledge and understanding of cybersecurity risks and threats, and to ensure that they are equipped with the necessary skills to recognize, prevent, and respond appropriately to various types of cyber threats.