Information Security Policy

Khon Kaen Sugar Industry Public Company Limited
and Group Companies

Information Security Policy

The key principles in this Information Security Policy are established as the framework for implementation to ensure the information technology systems of sugar companies in the KSL Group, which comprise:

1. Khon Kaen Sugar Public Company Limited
2. Thamaka Sugar Company Limited
3. New Krung Thai Sugar Factory Company Limited
4. New Kwang Soon Lee Sugar Company Limited
5. Savannahkhet Sugar Company Limited
6. Koh Kong Sugar Company Limited
7. Koh Kong Agriculture Company Limited
8. Khon Kaen Sugar Power Plant Company Limited
9. KSL Agro and Trading Company Limited
10. KSL Real Estate Company Limited
11. KSL Export Trading Company Limited
12. KSL Material Supplies Company Limited
13. Racha Churus Company Limited
14. Racha Ceramic Company Limited
15. Racha Porcelain Company Limited
16. Racha Products Company Limited
17. Chengpres Company Limited
18. Mae Sot Ceramic Limited Partnership
19. Racha Solar Material Company Limited

To ensure appropriate and efficient operations with security and stability, capable of continuously supporting the company's operations, as well as preventing potential problems arising from information technology system usage and various threats, based on the following principles:

1. Defining the scope of information security management with reference to the following requirements, laws, and best practices:
    1) Electronic Transactions Act B.E. 2544 (2001)
    2) Electronic Transactions Act (No. 2) B.E. 2551 (2008)
    3) Criteria for Retention of Computer Traffic Data by Service Providers B.E. 2550 (2007)
    4) Royal Decree on Secure Electronic Transaction Methods B.E. 2553 (2010)

5) Criteria and Methods for Preparing or Converting Documents and Text into Electronic Data Format B.E. 2553 (2010)
6) Computer Crime Act B.E. 2550 (2007)
7) ISO/IEC 27001 Standard

2. This policy must be disseminated to all relevant personnel at every level for acknowledgment.
3. This policy must be reviewed periodically once per year or when significant changes occur.

Furthermore, the Royal Decree on Secure Electronic Transaction Methods B.E. 2553 (2010) has declared that electronic transactions of agencies, companies, or units or companies that are considered critical infrastructure of the country must be conducted according to secure methods, whereby such electronic transactions shall be deemed to have been conducted according to reliable methods under Section 25 of the Electronic Transactions Act B.E. 2544 (2001), which the implementer must consider the following fundamental principles:

1. Confidentiality
2. Integrity
3. Available

As well as compliance with the company's policies and guidelines for operational control and information system security maintenance.

Policy Components

Definitions

"Security Maintenance"
Refers to the maintenance of security for the company's information technology and communication systems.

"Information Security"
Refers to the preservation of confidentiality, integrity, and availability of information, as well as other properties including authenticity, accountability, non-repudiation, and reliability.

"Data"
Refers to data and information in both document form and facts in various formats, such as data contained in company forms, including data in information systems, networks, computer equipment, or company data storage media, regardless of the format of such data. Reference to data under this definition shall include information as well.

"Assets"
Refers to data, programs, documents, equipment, tools, appliances, network system equipment, licensed software, and information technology systems that the company owns or has created and developed.

"User"
Refers to an authorized person who is permitted to use, manage, or maintain the company's information technology systems, with rights and responsibilities depending on their role.

System Administrator"
Refers to an employee appointed by the company group to perform duties of maintaining, servicing, and repairing computer equipment, as well as performing the function of granting user access rights to computer systems and network systems.

"External Entity"
Refers to a company or organization that the company authorizes to have rights to access and use the organization's data or various assets, whereby they shall receive usage rights according to their authority and must be responsible for maintaining data confidentiality.

"Data Owner"
Refers to a person authorized by a supervisor to be responsible for system data, whereby the data owner is responsible for such data or is directly affected if such data is lost.

"User Rights"
Refers to general rights, specific rights, special rights, and any other rights related to the organization's information systems.

"Password"
Refers to a group of text consisting of letters, numbers, or special characters designated for information system users to identify themselves and their rights to access information systems for the purpose of controlling data access.

"Information Access or Usage Control"
Refers to the authorization, rights assignment, or delegation of authority to users to access or use networks or information systems, both electronically and physically.

"Network System"
Refers to a system that can be used for communication or data and information transmission between various information technology systems of the company.

"Internet" refers to a global interconnected external network.

"Intranet" refers to the company's internal network.

"Electronic Mail"
Refers to a system that individuals use to send and receive messages between each other through computers and interconnected networks, where the transmitted data can include text, photographs, graphics, animation, and sound. The sender can send messages to a single recipient or multiple recipients.

"Undesirable Security Incident"
Refers to unwanted or unexpected security situations that may result in the company's systems being breached, attacked, or threatened.

"Supervisor"
Refers to an employee appointed by the company group to hold the position of head of a particular department in terms of operations, staff supervision, control, and ensuring operations comply with the company group's rules and regulations, as well as procedures established by higher-level supervisors.

Chapter 1

Data Backup and Recovery

Objectives

To ensure that data backup and system recovery operations are conducted appropriately and securely, while maintaining the accuracy and availability of information, as well as preventing unauthorized disclosure, modification, deletion, or destruction of data storage media.

Data Backup

1.1 Require the backup of critical business data to backup storage media, with the ability to recover data going back at least 7 days, including operating system programs, computer application programs, and complete command sets to ensure continuous availability.

1.2 Establish procedures or practices for data backup to serve as guidelines for operators, and require written approval documentation from authorized management personnel each time modifications are made to the data backup process (Job Backup).

1.3 Require daily logging of all operations related to data backup and data recovery by personnel to verify accuracy and completeness.

Data Recovery

1.4 Require testing of backup data at least once per year to ensure that data and various programs that are backed up are accurate, complete, and functional.

1.5 Establish procedures or practices for testing and implementing backup data from storage media, with data testing required before actual use to prevent data errors. Documentation must be prepared for data testing with signatures from all relevant data stakeholders or data users participating in every test.

1.6 When it is necessary to recover data from backup systems, regardless of the circumstances, written approval documentation from authorized management personnel must be obtained each time.

1.7 If damage occurs to database systems or network systems affecting service provision or system user operations, notify users (data owners) immediately, along with periodic progress reports on system recovery until completion.

1.8 In cases where data recovery affects data in other departments, notify the affected units before proceeding with system recovery.

Storage and Management of Recording Media

1.9 For high-importance systems, backup storage media along with copies of procedures or practices must be stored off-site for security purposes in case the current workplace becomes inaccessible.

1.10 There should be procedures for managing portable critical information storage media (External Hard Disk) in secure locations such as safes.

1.11 Clear identification labels with detailed information should be affixed to backup storage media to enable quick searches and prevent incorrect media usage.

1.12 There should be procedures for destroying critical data and unused storage media, including various critical data remaining in hard disk Recycle Bins.

Chapter 2

Information Systems and Network Operations

Objectives

To ensure that network operations are conducted appropriately and securely, capable of protecting software and information from destruction by unwanted programs, preventing unauthorized information processing on networks and supporting network infrastructure, and detecting unauthorized information processing, while enabling accurate monitoring, tracking, and authentication of individuals accessing information technology systems.

Data, Computer System, and Network Security

2.1 There is classification of data confidentiality levels, including control of access to each type of confidentiality level.

2.2 Transmission of critical data through public networks must be encrypted using international standards, such as SSL or VPN.

Server Computer System Security

2.3 There must be procedures or practices for checking computer system security, and when abnormal usage is detected, corrective action must be taken promptly.

2.4 Only necessary services must be enabled; if services pose security risks to the system, additional protective measures must be implemented.

2.5 System software patches must be installed regularly, such as for operating systems, database systems, various application programs, and developed web systems, to close various vulnerabilities.

2.6 Software related to security and general performance should be checked before installation and after correction or maintenance.

2.7 There should be guidelines for using security monitoring software such as Firewall, Personal Firewall, etc.

2.8 There must be clear designation of responsible persons for setting, correcting, or changing various program values, along with written approval documentation from authorized management personnel each time.

Network System Management and Monitoring

2.9 Networks must be segmented proportionally according to usage, such as Internal Zone, External Zone, and Demilitarized Zone (DMZ), etc.

2.10 There must be intrusion prevention systems such as Firewall or IDS, IPS between internal and external networks, etc.

2.11 There must be intrusion detection systems and abnormal usage monitoring through network systems, with regular monitoring required.

2.12 Security checks of computer equipment must be conducted before connecting to network systems, such as checking for computer system threats, verifying security parameter configurations, and physically disconnecting computers and disabling unnecessary ports.

2.13 In cases of Remote Access to network systems or external network connections using Client VPN, approval from authorized personnel is required with strict control, and authentic user identity verification must be performed.

2.14 Responsible persons must be clearly designated for setting, correcting, and changing various network system parameters and network connections, along with written approval documentation from authorized management personnel each time.

2.15 The use of various tools for network system checking should be approved by authorized personnel.

Software Installation, Modification, and System Performance Planning

2.16 Software installation must be done legally with proper licensing. The company does not permit employees to install any software that the company has not properly purchased according to law or performed without obligation.

2.17 Before changing systems and computer equipment, impact assessments should be conducted. After system changes, system operation checks should be performed and change records should be kept current, along with written approval documentation from authorized management personnel each time.

2.18 Computer system usage assessments should be conducted in advance to accommodate future usage.

Protection Against Computer System Threats and Malicious Code

2.19 Server computers and user computers connected to the network system must all have effective computer threat protection software installed and kept up-to-date.

2.20 Automatic virus scanning must be scheduled on user computers at 12:00 PM every working day, and virus signature database updates and Windows O/S patch updates must be maintained at all times.

2.21 The Computer Department must prepare a computer threat prevention manual for users to serve as practice guidelines, including method recommendations and providing users with knowledge about new types of computer threats.

2.22 There must be measures for preventing, controlling, and immediately suspending the use of unwanted software, along with immediate notification to relevant personnel when computer threats are detected.

Audit Logs

2.23 There must be logging of server computer and network operations, user application logs, and intrusion prevention system details, such as recording system access attempts, command line usage logging, and log file retention.

2.24 Usage access logging (computer traffic data) of users and system administrators must be maintained for at least 180 days.

2.25 There must be systems to prevent modification or alteration of various logs, and access rights to various logs must be limited to authorized personnel only.

Internet Usage

2.26 For internet usage, the company will consider granting permission based on necessity. Users must prepare approval documentation from their supervisors according to their work line, and after approval is granted, notify the system administrator to enable usage rights, while strictly complying with laws.

2.27 There must be consideration of content and services appropriate to usage necessity, at the discretion of supervisors according to the employee's work line.

2.28 Employees are prohibited from uploading or posting images or data containing computer system threats, data with unwanted command sets, or any data unrelated to the company on the company website and/or various websites that violate the Computer Crime Act B.E. 2550.

2.29 Employees are prohibited from downloading images or data containing computer system threats, data with unwanted command sets, or any data that violates the Computer Crime Act B.E. 2550 through the company's network system.

Electronic Communications

2.30 Information data size supported in electronic mail is limited to no more than 30 MB per transmission to support efficient usage.

2.31 Users should not send messages and file attachments exceeding 10 MB.

2.32 Electronic communications, whether email, messaging, or any other form of communication, shall be treated as formal correspondence and must comply with the company's document or letter sending and receiving regulations.

2.33 Employees should use polite language or language that the general public would appropriately use in messages sent to other persons, including proper compliance with customs and practices for electronic mail, conversations, or other electronic communications in network systems.

2.34 Employees are prohibited from sending false information, information that causes damage to the company or other persons, or sending images or messages related to obscene or indecent matters, or sending inappropriate messages such as vulgar language, profanity, or aggressive messages. In sending any information, employees must comply with the Computer Crime Act B.E. 2550, and the company reserves the right to monitor all electronic mail messages.

2.35 Employees are prohibited from performing any actions that violate the Computer Crime Act B.E. 2550 through the company's computer network system.

Social Media Usage

2.36 Publishing of company's important information, confidential information, company property data, including agreements, contracts, or contracts with business partners during operations is not permitted.

2.37 Conversations referencing the company should be avoided, and referencing the company in a manner that negatively impacts the company's image is not permitted.

2.38 Users should be cautious not to fall victim to unwanted programs.

2.39 In cases where the use of various social media platforms (such as Facebook, Twitter, Google+, Line, etc.) affects the performance of assigned duties, supervisors may set time periods to suspend usage.

2.40 The company reserves the right to monitor messages on various social media platforms that pass through the company's network system.

Chapter 3

Information Systems Access Control

Objectives

To control information system access to only authorized individuals, prevent unauthorized access, and provide protection against network intrusion from intruders and unwanted command sets that may cause damage to data or information technology system operations (Importance Level: High)

User Access Control

3.1 Data and computer system usage rights must be defined, such as computer application system usage and internet usage rights, whereby users must receive only the rights necessary for performing their duties and must receive written approval from authorized personnel.

3.2 In cases where users with special privileges are necessary, access usage must be strictly controlled.

3.3 In cases where it is necessary for users to be data owners and grant access rights to others, there must be specific individual or group designation only, with usage duration limits and immediate suspension upon expiration of the usage period.

3.4 Computer system usage rights and user registries must be reviewed at least once per year for security purposes.

Control of System Administrator Account and Password Usage

3.5 User: Administrator is designated as the User Account with the highest system privileges, and User: SA is designated as the User Account with the highest database system privileges, used for installation, correction, updating, and modification of operating systems and database systems respectively. Passwords must be securely stored as documents in sealed envelopes, with the Deputy Managing Director of Operations designated as the custodian, having the authority to co-sign the password document envelope with the Managing Director or another Deputy Managing Director.

3.6 If it is necessary to use User: Administrator and User: SA for any system corrections or modifications, approval documentation must be prepared on a case-by-case basis, with the Deputy Managing Director of Operations entering the password each time.

3.7 System checks must be conducted to change User: Administrator and User: SA passwords at least once per year, and whenever changes are made, passwords must be stored as documents in sealed envelopes as before.

Control of User Account and Password Usage

3.8 The company will provide User IDs and Passwords to employees whose duties involve using computer network systems and internet connections on an individual basis, with the following password usage rules:

3.8.1 Password length must be no less than 8 characters.

3.8.2 Characters can be used together in both uppercase and lowercase, and can be combined with special characters and numbers.

3.8.3 Personal user information cannot be used as passwords, such as first name, surname, birth date, employee ID, address, telephone number, etc.

3.8.4 Password change period is required within 90 days, and set passwords cannot be reused for 24 times for overall system security. Password entry errors are allowed no more than 5 times; if exceeded, the system will immediately lock the User Account and automatically unlock within 30 minutes. Users can request system administrators to unlock for usage.

3.8.5 There must be an identification and authentication system for users' identity verification and access rights before entering the computer system, with every user required to have their own User Account.

3.9 There must be control and management of system usage rights according to necessity, as users have obtained written approval from authorized management personnel.

3.10 Employee passwords are company property. Disclosing personal passwords to other persons is not permitted, and all employees have the duty to strictly protect company passwords.

3.11 The company does not permit shared usernames and passwords. Employees have the duty to be careful about network security, particularly not allowing other persons to access computer networks from their user accounts. To prevent others from learning and misusing employee passwords in ways that could damage the company, employees must keep passwords confidential and not use computer programs to automatically save passwords for personal computers in their possession.

3.12 Employees assigned to access various systems designated by the company must comply with system usage rules and keep usernames and passwords secure. Disclosure to others is prohibited except with written approval from direct supervisors.

3.13 If usernames and passwords need to be discontinued, notify direct supervisors to request discontinuation, which must be done immediately upon cessation of use.

3.14 In cases where employees resign, retire, or have reasons to leave work, supervisors have the duty to immediately request cancellation of that employee's username and password usage.

Control of Network System, Operating System, and Information System Access

3.15 There must be network identity verification, requiring network devices to be able to identify and authenticate themselves to indicate that the connection comes from authorized devices or locations.

3.16 Operating system access must have unique user identification and authentication without duplication.

3.17 Information system access must have restricted access to data and system functions according to the scope of authorized rights.

Chapter 4

Physical Security Implementation

Objective

To prevent unauthorized physical access and to prevent loss, damage, unauthorized disclosure of company assets, and disruption or interruption of the company's various operational activities (Importance Level: Medium)

Computer Center Access Control

4.1 Important computer equipment such as network equipment and server computers must be stored in secure areas.

4.2 There must be a personnel entry/exit monitoring system for the control room (Server Room) with strict monitoring, following the control room (Server Room) entry/exit regulations.

Damage Prevention

4.3 Computer rooms must have fire prevention equipment for computer rooms.

4.4 There must be backup power systems for computer rooms.

4.5 There must be air conditioning systems and humidity monitoring systems.

Chapter 5

Business Continuity Management

Objective

To prevent disruption or interruption of various business activities, focusing on protecting critical business processes from information system failures, and to enable system recovery within an appropriate timeframe (Importance Level: Medium)

Information Risk Management

5.1 Identify risks and critical risk events or sudden severe events that can lead to disruption or damage to information systems, for risk assessment purposes. Risk identification should address the following emergency scenarios:

- By event: Cases where buildings are sealed and access to the building is not possible
- By severity/area: Server Room fire, Information Department fire, building fire, flooding in building areas, company-wide system failure

5.2 Establish methods for assessing risks and severity of impacts.

5.3 Establish risk management measures, prepare or review problem-solving plans for uncertainties and disasters that may occur to information systems (IT Continuity Plan).

Chapter 6

Information Systems Procurement, Development, and Enhancement

Objective

To ensure that information system procurement and development consider security issues as fundamental components, to prevent errors in information system processing or unauthorized changes, and to create security for various system files (Importance Level: Medium)

System Development

6.1 Development Environment computers should be separated from Production Environment and controlled to allow access only to relevant personnel in each section.

6.2 Requesters and related users should participate in the development or modification process to ensure system development meets requirements.

6.3 Security and system availability should be considered from the beginning of development or modification.

6.4 Current detailed information about programs in use must be maintained, including details about past development, corrections, or changes.

6.5 All system documentation must be updated after development or modifications to remain current.

System Testing

6.6 Requesters, the Computer Department, and other related users must participate in testing to ensure that developed or modified computer systems operate efficiently and process completely and correctly.

6.7 Using actual operational data for system testing should be avoided. If necessary, protection and usage controls must be established.

Change Communication

6.8 Changes must be communicated to all relevant users comprehensively to ensure correct usage.

Chapter 7

Internal and External Information Security Infrastructure

Objective

To manage security services for information and processing equipment accessed by external entities within the company, and to ensure employees understand their roles and responsibilities, reducing risks arising from operational errors (Importance Level: Basic)

Service Provider Selection

7.1 There should be criteria for service provider selection, choosing service providers with thorough, rigorous, and trustworthy operational procedures.

7.2 There should be contracts that clearly specify data confidentiality.

7.3 There should be contracts that clearly specify implementation timeframes or problem resolution, work scope, and service conditions (Service Level Agreement).

Service Provider Control

7.4 In cases of using system development services, service providers must be limited to accessing only the Development Environment. If access to the Production Environment is required, strict control and monitoring of service providers must be implemented.

7.5 Service providers should be required to prepare operational manuals and related documents, with regular updates to keep them current.

7.6 Service providers should be required to report various problems and corrective approaches in their operations.

7.7 There should be procedures for accepting service provider deliverables.

Computer Security Incident Response

7.8 Define computer security violation incidents.

7.9 Prepare documentation for dissemination regarding computer security violation incidents.

7.10 Establish procedures for responding to various incidents, including monitoring and analyzing system attackers.

7.11 Define methods for data deletion and recovery.

Internal Company Security

7.12 There must be signed agreements between employees and the company that they will not disclose company secrets (this signing is part of employee hiring).

7.13 There should be independent auditor reviews of information security management, operations, and related practices.

Information Personnel Aspects

7.14 Written information security responsibilities should be defined for employees.

7.15 There must be disciplinary processes to punish violations of operating procedures.

7.16 Information access rights and information assets must be revoked upon termination of employment or change in employment nature.

Chapter 8

Information Asset Management

Objective

To protect company assets from potential damage and to appropriately define the level of company information protection (Importance Level: Basic)

Information Asset Management

8.1 An information asset inventory must be prepared, such as information data, information systems, information equipment, and others, with designation of asset importance levels and asset confidentiality for use in management consideration.

8.2 Designate information asset custodians.

8.3 Define appropriate levels of information asset protection.

Chapter 9

Information Security Incident Management

Objective

To ensure that information system security incidents and vulnerabilities receive appropriate action within suitable timeframes (Importance Level: Basic)

Information System Incident and Vulnerability Management

9.1 Records should be prepared and reports made on information system security vulnerabilities observed or suspected in systems or services in use.

9.2 Responsibilities and procedures should be defined to respond to incidents quickly and systematically.

9.3 Learning should occur from security breach incidents by considering causes, quantities involved, and costs from damages to prepare for future response.

Penalties

Employees have the duty to strictly comply. If any employee performs any action that constitutes a violation of such discipline, they will be subject to disciplinary punishment by the company group. The company group has established 4 types of disciplinary punishments as follows:

1. Verbal warning
2. Written warning
3. Suspension without pay for no more than 7 days
4. Termination without compensation and/or legal liability through prosecution

Criteria for Disciplinary Punishment Consideration

1. Disciplinary punishment consideration by verbal warning when the disciplinary violation shows the following results:
   - 1.1 The disciplinary violation has not yet caused harm to the company
   - 1.2 The violator has never committed the same violation before
   - 1.3 When the employee realizes they have committed a disciplinary violation and guarantees they will not violate again
   - 1.4 If any disciplinary violation has behavioral consequences different from any of these 3 criteria, punishment will be considered according to other penalty provisions. For punishment by verbal warning, once the supervisor has imposed the punishment, a record must be made of behavioral details, time, place, persons involved, and other details related to the employee's violation and sent to the Human Resources Department as quickly as possible.

2. Disciplinary punishment consideration by written warning, wage deduction, or suspension has the following punishment consideration criteria:
   - 2.1 When intentionally committing disciplinary violations or repeatedly violating the same discipline
   - 2.2 When the punishment reviewer determines that verbal warning punishment will not be effective, the following punishments shall be considered:
     - 2.2.1 Written warning
     - 2.2.2 Suspension from work

3. Disciplinary punishment consideration by termination without compensation will be imposed when an employee commits any of the following actions:
   - 3.1 Corruption in duty
   - 3.2 Intentionally committing criminal acts against the company group

3.3 Deliberately causing damage to the company group

3.4 Violating work regulations, rules, or lawful orders of the company group after receiving written warning, except in serious cases where the company group need not issue prior warning. The written warning is effective for no more than one year from the date the employee committed the violation

3.5 Abandoning duties for 3 consecutive working days, whether interrupted by holidays or not, without reasonable cause

3.6 Negligence causing serious damage to the company group

3.7 Receiving imprisonment sentence by final court judgment, except for penalties for violations committed through negligence or minor offenses

4. The consideration of punishment and penalties for disciplinary violations under the company group regulations as mentioned above are not yet detailed and comprehensive enough to cover all situations. Therefore, the consideration of punishment or determination of penalties shall be at the discretion of the company group, taking into account constructive approaches to ensure fairness and equality for all employees.

5. Additional Details Regarding Disciplinary Punishment

5.1 Warning validity period: Employees who commit disciplinary violations and receive verbal or written warnings shall have the warning remain effective for no more than one year from the date the employee committed the violation.

5.2 When a single action violates multiple regulations, the regulation with the heaviest penalty shall be applied to punish the violator.

5.3 Multiple violations in consecutive time periods: When an employee commits multiple violations in consecutive time periods, even though the company group may have immediately implemented disciplinary punishment, it may not keep pace with events because other violations have been committed in consecutive time periods. In this case, the company group may consider imposing disciplinary punishment heavier than the penalty for the violation considered most serious among the violations the employee has committed.

5.4 During disciplinary consideration, the company group has the right to suspend employees for investigation for no more than 7 days, paying fifty percent of wages. When the investigation is completed, if it appears the employee is not at fault, the company group will pay the employee wages equal to working day wages from the date the employee was ordered suspended.

6. Authority to Consider and Implement Disciplinary Punishment

6.1 For punishment, the direct supervisor of the employee who committed the violation, together with a supervisor one level higher, shall consider and implement the punishment.

Appendix 1

Duties and Responsibilities of Information Personnel

To ensure orderly use of computer systems and to clearly define the duties and responsibilities of company personnel in their work performance, which include the following responsibilities:

1. The Company Managing Director has the following duties:
   - 1.1 Oversee and be responsible for the performance of duties of all personnel in the company to respond to company policies
   - 1.2 Establish policies and operating principles
   - 1.3 Have authority to approve company principles and expenses
   - 1.4 Oversee and monitor progress and evaluate results at all levels and all departments in KSL IT Center Company Limited
   - 1.5 Have authority to punish employees who violate various rules and regulations of the company group, whether intentional or unintentional, by adhering to the company's punishment guidelines
2. The Deputy Managing Director has the following duties:
   - 2.1 Oversee and be responsible for the work performance of all personnel in the computer systems line to respond to company group policies
   - 2.2 Have authority to approve principles and expenses within the responsible department within the allocated budget or submit matters to the company board meeting for approval consideration
   - 2.3 Plan and prepare budgets within the computer systems department for presentation to management. Once received, must coordinate with various department managers to control and oversee various expenses to align with the received budget and achieve maximum efficiency
   - 2.4 Oversee and monitor progress and evaluate work performance at all levels and all departments in the line of work
   - 2.5 Analyze and evaluate work performance of all personnel in the line of work twice per year
   - 2.6 Punish employees in the responsible line of work in cases of violating various rules and regulations of the company group, whether intentional or unintentional, by adhering to the company's punishment guidelines according to company regulations
3. The Application Development Department Manager has the following duties:
   - 3.1 Oversee and be responsible for the performance of duties of all personnel in the Application Development Department to respond to company group policies
   - 3.2 Plan and manage budgets within the Application Development Department for presentation to management. Once the budget is received, the Application Development Department Manager must control and oversee various expenses that arise to align with the received budget and achieve maximum efficiency

3.3 Oversee and monitor progress and evaluate the performance of various system implementations of all project personnel, while providing necessary assistance for project advancement

3.4 Analyze and evaluate work performance of all personnel in the Application Development Department twice per year

3.5 Oversee, procure, and prepare various necessary tools and equipment within the Application Development Department

3.6 Punish employees within the Application Development Department who violate various rules and regulations of the company group, whether intentional or unintentional, by adhering to the punishment guidelines according to company group regulations

4. The Application Development Department Assistant Manager, Computer System Development Section, has the following duties:

4.1 Control and oversee various tasks in computer system development to ensure accuracy, completeness, and timely completion according to the planned schedule

4.2 Control and oversee the storage of source programs and various versions of each computer system used in the company group

4.3 Control and oversee the preparation and storage of databases for various computer systems used in the company group

4.4 Design and prepare various standard documents used in computer system development

4.5 Study and research new tools to help develop computer systems more conveniently and rapidly

4.6 Develop computer work and test various sub-programs as assigned from the system consulting section

4.7 Analyze and evaluate work performance of all personnel in the computer system development section twice per year

5. The Application Development Department Assistant Manager, System Consulting Section, has the following duties:

5.1 Control and oversee various tasks in the system consulting section, both project work and support work, to ensure accuracy, completeness, and completion according to the planned schedule

5.2 Control and oversee the preparation of manuals and various documents accompanying computer work

5.3 Control and oversee computer system training for various systems in the company group

5.4 Schedule and plan visits to survey various requirements of system users in each company

5.5 Study and research new computer systems that are beneficial and add value to present to each company group

5.6 Design overviews and details, including prepare documentation for modifying existing computer systems or creating new computer systems for delivery to the computer system development section to use in further system development

5.7 Analyze and evaluate work performance of all personnel in the system consulting section twice per year

6. Computer System Development Personnel have the following duties:

6.1 Develop computer systems and test various sub-programs to ensure accuracy, completeness, and timely completion according to the schedule for work received from the system consulting section

6.2 Store source programs and various versions of each computer system for which they are responsible

6.3 Prepare and store computer system databases for greater convenience and speed

7. Computer System Development Personnel have the following duties:

7.1 Collect and gather data to thoroughly study various requirements of computer system users in detail

7.2 Design overviews and details, including prepare documentation for modifying existing computer systems or creating new computer systems for delivery to the computer system development section to use in further system development

7.3 Test the entire system program to verify whether it meets user requirements

7.4 In cases where program errors are found or it is discovered that it does not meet user requirements, schedule appointments with the program manufacturer or computer system development section to consult and discuss approaches for problem resolution

7.5 Prepare manuals and various documents accompanying computer systems for which they are responsible

7.6 Prepare documents and computer equipment, programs, and databases for which they are responsible for use in training system users

7.7 Conduct training for all relevant users in modifying existing computer systems or creating new computer systems

7.8 Arrange periodic meetings at least twice per month to monitor progress and resolve problems promptly

7.9 Provide care and consultation regarding various computer systems to users in cases where users encounter usage problems

8. The Infrastructure Manager has the following responsibilities:

8.1 Supervise and assume responsibility for all operational activities of Infrastructure Department personnel to align with corporate group policies.

8.2 Plan and prepare budgets for the Infrastructure Department for presentation to management. Upon budget approval, the Infrastructure Manager must control and monitor all expenses to ensure compliance with the allocated budget and achieve maximum efficiency.

8.3 Monitor and track progress, and evaluate the performance of system planning work by all plant personnel, while providing necessary assistance for project advancement.

8.4 Analyze and assess the performance of all Infrastructure Department personnel twice annually.

8.5 Oversee, procure, and prepare necessary tools and equipment within the Infrastructure Department.

8.6 Discipline employees within the Infrastructure Department who violate corporate group regulations, whether intentionally or unintentionally, in accordance with the company's disciplinary guidelines.

9. The Assistant Infrastructure Manager for Network Systems and Security has the following responsibilities:

9.1 Oversee and procure network equipment necessary for network systems within the Infrastructure Department and group companies, subject to approval from the Infrastructure Manager.

9.2 Maintain network equipment to ensure continuous operational readiness at all times.

9.3 Plan backup equipment requirements to prevent network system interruptions.

9.4 Plan and design comprehensive networks for the entire corporate group, both current and future, to support corporate advancement.

9.5 Assign IP addresses to all servers and client machines within the company.

9.6 Conduct daily network system inspections to ensure consistent normal operations, while analyzing and optimizing network systems for maximum efficiency.

9.7 Oversee and prepare modern computer threat protection software systems for company implementation, with continuous updates to maintain currency.

9.8 Authorize Internet access privileges for users within the corporate group based on access request documentation approved by respective department managers and the Infrastructure Manager.

9.9 Provide guidance to computer departments of various companies within the group to implement standardized computer threat protection systems, ensuring uniform standards and confidence in network security against computer threats.

9.10 Oversee and prepare Internet and Intranet network systems for company implementation, with continuous modernization updates.

9.11 Oversee and prepare IP Voice/IP Phone, Video Conference, and CCTV systems for company implementation, with continuous modernization updates.

9.12 Oversee, procure, and prepare Network Monitoring systems for company implementation, with continuous modernization updates.

9.13 Upon detection of abnormal communication system usage (attacks from internal or external computers), immediately provide written notification to the Infrastructure Manager or report to the Deputy Managing Director of Computer Operations.

9.14 Perform duties as assigned by management and implement corrective measures for network system malfunctions.

9.15 Upon observing users violating corporate group computer usage regulations and/or illegal software usage, prepare written documentation to notify the Infrastructure Manager or report immediately to the Deputy Managing Director of Computer Operating Systems.

10. The Assistant Infrastructure Manager for Computer Systems has the following responsibilities:

10.1 Oversee, procure, and prepare email systems for all requesting users, subject to written documentation approved by their direct supervisors and authorized by the Infrastructure Manager.

10.2 Assign usernames and passwords to all network system applicants who have properly completed application documentation and received approval from the Infrastructure Manager.

10.3 Configure database access privileges for all users according to approvals received from respective departmental management.

10.4 Perform daily company data backup to Storage Disk systems at least once daily after 24:00 hours to prevent user work interruptions.

10.5 Conduct regular and systematic scanning and elimination of computer threats on server systems.

10.6 Provide guidance to computer departments of various companies within the group to implement standardized computer threat protection software, ensuring uniform standards and confidence that the corporate group's network systems are secure from computer threats.

10.7 Plan and conduct verification procedures to ensure that backup data systems can be utilized when required.

10.8 Prepare server computer systems for future projects upon written request from project managers through the Deputy Managing Director of Computer Operating Systems.

10.9 In case of server problems, the Assistant Infrastructure Manager for Computer Systems must immediately notify the Hardware Manager, Software Manager, and respective project managers to consult and determine solutions for transferring problematic systems or databases to backup servers. Upon reaching conclusions, corrective actions must be implemented immediately to restore normal operations.

11. The Database System Administrator has the following responsibilities:

11.1 Install and configure Database Servers for various computer system databases used within the corporate group.

11.2 Set up Job Replicate Data and Job maintenance Database for various computer system databases.

11.3 Monitor and maintain all jobs on database servers to ensure normal operations on a daily and consistent basis.

11.4 Monitor and maintain available space on database servers to enable daily database backups.

11.5 Plan and conduct inspections every 3 months to ensure that backup databases can be utilized when required.

11.6 Analyze and resolve various problems occurring with database servers of computer systems.

11.7 In case of data problems, the Database Administrator must immediately notify the Software Manager and respective project managers to consult and determine solutions for problematic databases. Upon reaching conclusions, the Database Administrator must immediately implement corrective actions to restore normal operations.

11.8 Control and maintain security systems on database servers for various computer system databases.

11.9 In cases of unauthorized database access, whether intentional or unintentional and by any means, the Database Administrator must immediately issue a written warning to the violator's supervisor and provide written notification to the Software Manager.

11.10 Control and maintain the preparation of manuals and documentation for database server administration.

11.11 Study and research new database technologies for implementation within the corporate group.

12. The Network Systems and Security Officer has the following responsibilities:

12.1 Prepare written documentation in cases where any user or users have violated computer usage regulations, whether intentionally or unintentionally, to notify the respective employee(s).

12.2 Authorize Internet access privileges for users within the corporate group who have completed access request documentation approved by respective department managers and authorized by the Infrastructure Manager.

12.3 Monitor and inspect data communication systems between various sites to ensure normal operations on a daily and consistent basis.

12.4 Upon detection of abnormal communication system usage (attacks from internal or external computers), immediately provide written notification to the Infrastructure Manager or report to the Deputy Managing Director of Computer Operations.

12.5 Perform duties as assigned by the Assistant Manager for Network Systems and Security, including correcting network system malfunctions as delegated.

12.6 Upon observing users violating corporate group computer usage regulations and/or illegal software usage, prepare written documentation to notify the Assistant Manager for Network Systems and Security and the Infrastructure Manager, or report immediately to the Deputy Managing Director of Computer Systems.

12.7 Assist in overseeing and procuring equipment or software for network security maintenance, ensuring readiness and continuous modernization.

13. The Computer Systems Administrative Officer has the following responsibilities:

13.1 Install computer systems for all users within the corporate group who have completed access request documentation and received approval from the Infrastructure Manager and/or Assistant Manager for Computer Systems.

13.2 Configure various computer system settings as assigned by the Network Systems Manager or Assistant Manager for Computer Systems.

13.3 Maintain and troubleshoot computers in the network system to ensure normal operational capability.

13.4 Conduct regular and systematic scanning and elimination of computer threats in the network system.

13.5 Perform duties as assigned by supervisors to correct computer system malfunctions and network equipment issues.

13.6 Maintain and service backup power system equipment including UPS and generators.