# Corporate Governance Policy

Presented by the Board of Directors

2nd Revised Edition, dated October 7, 2025

## Vision

Principal Capital Public Company Limited will be an organization focused on expanding its business in the healthcare sector. The company will be recognized as an expert in hospital management, known for leveraging technology to enhance service quality and efficiency. Additionally, the company will fully utilize other real estate properties it owns to maximize benefits for all stakeholders.

## Mission

- The Company will provide professional hospital management services and support functions to both its network hospitals and partner hospitals that have been given the opportunity for management.
- The Company will be committed to managing hospitals efficiently by leveraging technology to achieve set goals, including financial performance, service quality, and customer satisfaction.
- The Company will dedicate itself to continuously developing its personnel to enhance their technological capabilities and new skills, ensuring they can support the rapid growth of the organization.
- The Company will strengthen its hospital network by forming partnerships and/or acquiring other businesses to jointly enhance capabilities and improve performance.
- The Company will seek new health-related projects to further expand its business.
- The Company will be a part of driving and elevating community healthcare to create a sustainably healthy society.

# Corporate Governance Policy

## Message from the Chairman of the Board of Directors

The Company is committed to becoming a leading corporation in its industry, both nationally and regionally, enhancing organizational value and promoting business operations in compliance with applicable laws and corporate ethics to achieve stable and sustainable growth with integrity, morality, transparency, fairness, and a steadfast opposition to corruption. These fundamental values of a leading organization build trust among investors, employees, business partners, competitors, creditors, stakeholders affected by the Company's operations, and benefit Thai society and the environment through business management aligned with internationally recognized corporate governance standards, enabling the organization to achieve its goals of becoming a sustainable enterprise with good governance.

The Board of Directors recognizes the importance of good corporate governance and has approved this "Corporate Governance Policy" to serve as a guideline for best practices for all directors, executives, and employees to:

1. Apply the Company's corporate governance principles in business management at all levels;
2. Uphold fairness in treating shareholders, stakeholders, society, and the environment equitably, and perform their duties in the best interests of the Company to the fullest extent of their abilities with integrity, transparency, and accountability;
3. Use this policy as a key indicator for evaluating the Board of Directors' and executives' business management performance, as well as the work performance of all employees.

(Mr. Chanin Khaochan)

Chairman of the Board of Directors

Principal Capital Public Company Limited

## Table of Content

## Guidelines for Compliance with the "Corporate Governance Policy"

1. Learn, understand, and review the "Corporate Governance Policy Manual" as it relates to one's duties and responsibilities.
2. Provide knowledge and understanding to other individuals when performing duties that may involve the Company or may have an impact on the Company.
3. When in doubt or having questions, consult with one's supervisor or the Company Secretary, who is responsible for monitoring compliance with the "Corporate Governance Policy Manual."
4. Report to one's supervisor or the Company Secretary when violations or non-compliance with the "Corporate Governance Policy Manual" are observed.
5. Cooperate in fact-finding investigations with relevant departments or the Company Secretary.
6. Supervisors at all levels must lead by example in complying with the "Corporate Governance Policy" and foster a work environment that ensures employees and relevant individuals understand that compliance with the "Corporate Governance Policy" is both proper and mandatory.

## Monitoring and Ensuring Compliance with the "Corporate Governance Policy"

The Company will not engage in any actions that violate the law or contradict the Company's "Corporate Governance Policy." It is the duty and responsibility of all directors, executives, and employees to acknowledge and comply with the policies and requirements set forth in the Company's "Corporate Governance Policy." Furthermore, executives at all levels must oversee and take responsibility for promoting knowledge, understanding, and strict compliance with the Company's "Corporate Governance Policy" among employees under their supervision, as this is considered a matter of utmost importance.

Should any director, executive, or employee violate the Company's "Corporate Governance Policy," they will be subject to strict disciplinary action. If there are actions that are reasonably believed to violate laws, rules, regulations, and government requirements, the Company will refer the matter to the relevant government authorities for further action.

## Guidelines for Reporting Concerns

To ensure fairness and equal treatment of all stakeholders in accordance with the "Corporate Governance Policy," the Company has established channels for reporting concerns, complaints, comments, or suggestions indicating that stakeholders have been affected or are at risk of being affected in a manner that may cause harm to any stakeholder group from the Company's business operations or from the conduct of the Company's directors, executives, and employees regarding violations of laws or ethics, including behavior that may suggest fraud, unequal treatment, or actions lacking caution and prudence. Concerns may be reported directly or by contacting:

1. For External Parties, contact the Company Secretary

   Website : Contact Us at www.principalcapital.co.th

   Telephone : 02-009-2015

   Email : Princ_secretarywhistle@princgroup.com

   Mail : Company Secretary
   Principal Capital Public Company Limited
   29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63,
   Khlong Tan Nuea, Watthana, Bangkok 10110

2. For Employees, contact the Internal Whistleblowing Committee

   Email : Princ_internalwhistle@princgroup.com

   Mail : Internal Whistleblowing Committee
   29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63,
   Khlong Tan Nuea, Watthana, Bangkok 10110

## Whistleblower Protection Measures

The Company has established guidelines whereby those assigned to receive concerns shall maintain confidentiality of relevant information and shall disclose only as necessary, taking into consideration the safety and potential harm to the reporter or those cooperating in the investigation. The Company guarantees that such reporting will not constitute grounds for termination, disciplinary action, or any adverse action against such employees. Whistleblowers may choose not to disclose their identity if they believe disclosure would be unsafe; however, self-identification will enable the Company to provide progress reports, clarify facts, or mitigate actual damages more conveniently and expeditiously. Those who have suffered harm will receive remediation through appropriate and fair processes.

The Company establishes its operational systems and internal controls in accordance with the aforementioned corporate governance principles, which comprise the following key elements:

## Section 1: Shareholder Rights

- Shareholders have ownership rights and the right to oversee the Company's affairs through the appointment of the Board of Directors.
- Shareholders have the right to participate in decisions regarding significant changes to the Company.
- Shareholders should receive documents and details for attending shareholder meetings in a timely manner.
- Shareholders should have the opportunity to propose meeting agenda items and have the right to appoint proxies to attend meetings on their behalf.
- The Company should promote the exercise of shareholder rights and shall not violate or infringe upon shareholder rights.

The Company recognizes and attaches importance to shareholder rights and has therefore established the following guidelines to safeguard shareholder rights:

1. The Company shall send notices convening Annual General Meetings and Extraordinary General Meetings, clearly specifying the venue, date, and time of the meeting, together with detailed meeting agendas, material information necessary for consideration, the Board of Directors' opinions, minutes of the previous meeting, the annual report, proxy forms (Forms A, B, and C available for selection), and clear proxy instructions to facilitate and encourage shareholders, including institutional investors, to attend meetings. The Company shall deliver meeting documents to shareholders at least 21 days prior to the shareholder meeting date and shall publish such information in advance on the Company's website in both Thai and English at www.principalcapital.co.th at least 30 days prior to the meeting date to ensure shareholders receive accurate, complete, transparent, and sufficient information for decision-making and voting, and to prepare proxy appointments in cases where personal attendance is not convenient.

2. The Company has a policy to promote and facilitate shareholder and institutional investor participation in shareholder meetings. The Company shall schedule meetings at appropriate dates and times, arrange meeting venues of adequate size to accommodate attending shareholders with sufficient access to public transportation for convenient travel, and provide venue maps, as well as ensure adequate personnel and technology for document verification and voting.

3. The Company shall announce details of the Annual General Meeting in newspapers in both Thai and English for three consecutive days, at least three days prior to the meeting date, and shall publish such information on the Company's website in both Thai and English at www.principalcapital.co.th as advance notice of the Annual General Meeting.

4. The Company shall not undertake any action that restricts shareholders' rights to attend meetings. All shareholders have the right to attend shareholder meetings throughout the duration of the meeting, the right to ask questions,

express opinions to the meeting on agenda items and proposed matters, and vote on meeting agenda items. The Chairman of the meeting should allocate time appropriately and encourage the expression of opinions and questions during the meeting.

5. The Company has established guidelines for the Annual General Meeting agenda to comply with good corporate governance principles as follows:

   5.1 Approval of minutes of the previous meetingรับรองรายงานการประชุมครั้งที่ผ่านมา

   5.2 Acknowledgment of the Company's operating results for the past year

   5.3 Consideration and approval of the statement of financial position and statement of comprehensive income for the accounting period ending December 31 of the previous year

   5.4 Consideration and approval of profit allocation from the previous year's operating results

   5.5 Consideration and election of directors to replace those retiring by rotation

   5.6 Consideration and approval of directors' remuneration

   5.7 Consideration and appointment of auditors and determination of annual audit fees

   5.8 Other matters

The Company provides shareholders the opportunity to ask questions on important matters of interest and/or the Board of Directors answers questions and/or provides clarification to shareholders without voting.

6. The Company provides shareholders the opportunity to propose meeting agenda items in advance and nominate individuals for consideration as Company directors for a period of no less than three months annually, at least three months prior to the shareholder meeting date, by submitting original documents by mail to the Company Secretary as detailed on the Company's website.

7. The Company provides shareholders the opportunity to submit questions related to shareholder meeting agenda items to the Board of Directors in advance, at least 10 days prior to the shareholder meeting date, through the Company's website, fax, or the Company Secretary's email.

8. The Company prepares and publishes shareholder meeting minutes to the Stock Exchange of Thailand within 14 days following the meeting date in accordance with the Stock Exchange of Thailand's requirements, comprehensively and appropriately, including detailed recording of meeting minutes, voting results, and shareholder questions for each agenda item.

9. All Company directors, including members of specific committees/subcommittees/working groups, the Chief Financial Officer or Chief Accounting Officer, and the Company Secretary must attend all shareholder meetings unless unavoidably prevented by important commitments, in order to answer questions and hear shareholder opinions. All senior executives should also attend shareholder meetings to answer questions.

## Section 2: Equitable Treatment of Shareholders

- All shareholders, both major and minority shareholders, should receive equitable and fair treatment.
- The Company should ensure that shareholders receive equitable treatment and protection of their fundamental rights.

The Company has ethics regarding confidentiality and the use of inside information, with guidelines for oversight to protect shareholders' fundamental rights equitably and fairly, building confidence in investing with the Company, as follows:

1. The Company provides shareholders the opportunity to propose matters for inclusion as agenda items at shareholder meetings and to nominate individuals for election as directors in accordance with the criteria established by the Company, which are published on the Company's website at www.principalcapital.co.th. Proposals must be submitted to the Company for at least one month annually, at least three months in advance of the shareholder meeting date, by sending original documents by mail to the Company Secretary as detailed on the Company's website. The Board of Directors will disclose the results of such considerations through the Company's website and the Stock Exchange of Thailand's website.
2. The Company shall not add meeting agenda items or change material information without providing advance notice to shareholders.
3. Shareholders have the right to appoint proxies to attend meetings and vote on their behalf. Shareholders have the right to receive documents and guidance on proxy appointments. Proxies who are legally authorized and submit proxy documents to the directors at the meeting have the right to attend the meeting and vote in the same manner as shareholders in all respects. Shareholders may appoint the Company's independent directors to attend the meeting and vote on their behalf. Shareholders have the right to receive comprehensive and appropriate profiles and work information for each independent director for their consideration.
4. The Board of Directors provides shareholders the opportunity to exercise their right to appoint directors individually and supports the use of transparent, convenient, efficient, and expeditious voting methods and equipment that can promptly display voting results, enabling shareholders to know the voting outcomes in a timely manner.
5. Directors and executives must disclose information regarding interests and related parties to enable the Board of Directors to consider the Company's transactions that may involve conflicts of interest or connected transactions and make decisions in the best interests of the Company as a whole. Directors and executives with interests in transactions conducted with the Company must not participate in decisions regarding such transactions, in accordance with the procedures or approval measures for the Company's related party transactions.

## Section 3: Role Toward Stakeholders

- The Company protects stakeholders' rights in accordance with applicable laws and considers promoting cooperation between the Company and stakeholders in creating wealth, financial stability, and business sustainability.
- The Company has established measures for receiving complaints, comments, and suggestions, as well as reporting suspected violations of law or ethics that may indicate fraud or misconduct by employees and other stakeholders of the Company.

The Company has provided care and consideration for all stakeholder groups, taking into account the rights of stakeholders under law or agreements with the Company, and has clearly defined guidelines for oversight of roles toward each stakeholder group for employees at all levels to follow as an important duty of everyone, as follows:

1. The Company's stakeholders include customers, employees, business partners, shareholders or investors, creditors, competitors, society and the environment, government agencies, and related organizations. For each of these groups, the Company must provide adequate channels for communication and response to the needs of each group from the Company.
2. The Company is committed to customers in continuously developing and improving products and services, establishing prices appropriate to the situation, and not engaging in any actions that take advantage of customers. In dealing with business partners, the Company must conduct business in a neutral and fair manner.
3. The Company is mindful of employee welfare by not taking advantage in employment contracts, establishing remuneration appropriate to capabilities to motivate employees in their work, providing training and continuing education to enhance employee potential, maintaining a good work environment, establishing safety standards, creating work discipline, and providing thorough care and attention. The Company has established remedial plans for those affected should employees need to terminate their employment for any reason.
4. The Company continuously and regularly communicates to raise awareness and demonstrate care for stakeholders.

## Section 4: Information Disclosure and Transparency

- The Board of Directors should ensure that the Company discloses material information relating to the Company, both financial and non-financial information, accurately, completely, timely, and transparently through channels that provide easy access to information with equality and credibility.
- The Board of Directors should establish a department or designate a responsible person for external communications to communicate with investors, such as institutional investors or shareholders, and other related organizations on an equitable basis.

The Company places importance on the disclosure of material information that is accurate, complete, precise, and timely for stakeholders to use in making decisions. Information disclosure is an indicator of transparency in operations, which is a critical factor in building confidence among shareholders, investors, and stakeholders regarding the integrity of operations and serves as a mechanism for monitoring operations. The Company has therefore established the following guidelines for oversight of information disclosure and transparency:

1. The Board of Directors, or those authorized by the Board of Directors, are responsible for disclosing information, both financial and non-financial, adequately, reliably, and in a timely manner to ensure that the Company's shareholders and stakeholders receive information equitably as required by law and the Company's regulations, and to ensure that information on the website is updated comprehensively, regularly, promptly, and in accordance with current situations, to ensure that shareholders can obtain additional information for consideration and contact the department responsible for providing information conveniently, quickly, and efficiently.
2. The Company's information system is carefully prepared with clarity, accuracy, and transparency using concise and easy-to-understand language, with regular disclosure of material and necessary information regardless of whether it has a positive or negative impact on the Company.
3. The Company establishes a public relations department to perform public relations functions for information, news, operations, and performance of the Company that is beneficial to shareholders, investors, employees, related parties, and the general public regularly and efficiently, eliminating misunderstandings. The Company also has an investor relations function to serve as a liaison with institutional investors, creditors, securities analysts, and the Company's shareholders in providing information on the Company's operations and investments through convenient, quick, and easily accessible contact channels.
4. The Board of Directors arranges for the preparation of the statement of financial position and statement of comprehensive income, and the audit report of the auditor, to be accurate in accordance with accounting standards and laws, together with the Board of Directors' annual report on the accuracy, completeness, and adequate disclosure of material information in the statement of financial position and statement of comprehensive income, to be presented to the shareholder meeting at the Annual General Meeting for consideration and approval.

5. The Board of Directors prepares a report assessing the Company's status and outlook in an easy-to-understand summary, a report describing its responsibility for preparing financial reports, displayed alongside the auditor's report, and reports on directors' and/or audit committee members' meeting attendance compared with the number of Board of Directors' and/or Audit Committee meetings held each year in the annual report.

6. The Board of Directors has arranged for reporting of changes in securities holdings of the Company's directors and executives in accordance with the regulations of the Securities and Exchange Commission and the Stock Exchange of Thailand.

## Section 5: Responsibilities of the Board of Directors

- The Board of Directors plays a critical role in corporate governance for the best interests of the Company.
- The Board of Directors is accountable for the performance of its duties to shareholders.
- The Board of Directors must be independent from the Company's management.

The Company has guidelines for oversight of the Board of Directors' responsibilities, whereby the Board of Directors must comprise individuals with knowledge, expertise, and experience capable of benefiting the Company, demonstrating dedication and devoting sufficient time to perform their responsibilities. The Board of Directors is appointed by shareholders to govern the direction of the Company's operations. The Board of Directors appoints management to be responsible for business operations and appoints specialized committees to be responsible for specific assigned matters, nominates auditors for shareholder approval and appointment, and appoints the Company Secretary to be responsible for conducting meetings and compliance with laws.

The guidelines for oversight of the Board of Directors' responsibilities are as follows:

1. Composition and Qualifications of Company Directors
2. Specialized Committees / Subcommittees / Working Groups
3. Independent Directors and Qualifications of Independent Directors
4. Powers, Duties, and Responsibilities of the Board of Directors
5. Powers, Duties, and Responsibilities of the Audit Committee
6. Powers, Duties, and Responsibilities of the Nomination and Remuneration Committee
7. Powers, Duties, and Responsibilities of the Executive Committee
8. Powers, Duties, and Responsibilities of the Corporate Governance Committee
9. Powers, Duties, and Responsibilities of the Sustainable Development Committee
10. Powers, Duties, and Responsibilities of the Risk Management Committee
11. Board of Directors' Meetings
12. Appointment and Removal of Company Directors
13. Performance Evaluation of the Board of Directors
14. Remuneration of Directors and Chief Executive Officer
15. Development of Directors and Executives

## 1. Composition and Qualifications of Company Directors

1.1 Must possess the qualifications and not have any prohibited characteristics under the Public Limited Companies Act, and must have knowledge, capability, expertise in business, and relevance to the business.

1.2 The Board shall consist of at least five (5) members, with not less than half of the total number of directors residing in Thailand. Directors may or may not be shareholders of the Company.

1.3 The appointment of directors must follow specifically designated agenda items with transparency and clarity, and must include the individual's profile with sufficient details to benefit the shareholder meeting's decision-making. The profiles of all Company directors must be disclosed in the annual report for the general knowledge of shareholders.

1.4 The Board of Directors must have at least three independent directors, comprising not less than one-third of the entire Board of Directors. Independent directors may serve a term of office not exceeding nine years.

1.5 Each Company director may hold directorships in no more than five listed companies.

**Role and Duties of the Chairman of the Board of Directors**

The Company stipulates that the Chairman of the Board of Directors and the Chief Executive Officer of the Company shall not be the same person. The Chairman of the Board of Directors has the following roles and duties:

1. Convene Board of Directors' meetings, chair Board of Directors' meetings and shareholder meetings, and play a role in establishing meeting agendas jointly with the Board of Directors.
2. Play a role in controlling Board of Directors' and shareholder meetings to ensure efficiency and successful completion in accordance with the Company's regulations.
3. Support and provide opportunities for Company directors to express opinions independently and equally.
4. Support and promote the Board of Directors in performing their duties to the fullest extent within the scope of their powers, duties, and responsibilities, and in accordance with good corporate governance principles.
5. Oversee and monitor the administrative work of the Board of Directors and other sub-committees to achieve their established objectives.
6. Cast the deciding vote in cases where the Board of Directors' meeting votes and the votes on both sides are equal.

## 2. Specialized Committees / Subcommittees / Working Groups

### 2.1 Audit Committee

The Audit Committee shall consist of at least three independent directors, with at least one member possessing sufficient knowledge and experience to review the reliability of financial statements. The Audit Committee must possess qualifications regarding independence in accordance with the notifications of the Securities and Exchange Commission and the Stock Exchange of Thailand regarding qualifications and scope of operations of the Audit Committee to perform duties of auditing and overseeing the Company's operations, overseeing financial reports, internal control systems, selection of auditors, consideration of conflicts of interest, and risk management. The Audit Committee shall possess the following qualifications:

1. Must be independent directors and appointed by the Board of Directors.
2. Must be directors who are not employees, staff, or consultants receiving regular salaries from the Company, parent company, subsidiaries, associated companies, and related companies.
3. Must be individuals who are trusted and generally accepted, and able to devote sufficient time to perform the duties of the Audit Committee.

*Note: Other important qualifications shall comply with the qualifications of independent directors as prescribed by the SET and SEC (Manual page 26) and the Audit Committee Charter, which can be downloaded from the Company's website.*

### 2.2 Nomination and Remuneration Committee

The Nomination and Remuneration Committee shall comprise at least two Company directors, with at least two members being independent directors, and the Chairman of the Nomination and Remuneration Committee should be an independent director. Even if some positions become vacant, the remaining directors may continue to conduct business; however, if the number of directors decreases to the point where it is insufficient to constitute a quorum, the remaining directors may only conduct business by arranging a meeting to appoint additional directors to replace all vacant positions. The Nomination and Remuneration Committee shall possess the following qualifications:

1. Must possess knowledge, capability, and experience, as well as knowledge and understanding of the qualifications, duties, and responsibilities as a member of the Nomination and Remuneration Committee.
2. The Chairman of the Nomination and Remuneration Committee should be an independent director to serve as a key driver to ensure the performance of duties of the Nomination and Remuneration Committee is conducted independently.

### 2.3 Executive Committee

The Executive Committee must be appointed by the Board of Directors and consist of at least three members, including at least one Company director, performing the following duties:

1. Screen policies, direction, business strategies, management structure, business plans, and annual budgets.
2. Monitor and oversee the implementation of:
    2.1 Strategic plans, work plans, and projects within the annual business plan approved by the Board of Directors
    2.2 The Company's financial operating results, and
    2.3 Consider investments and risk management.
3. Perform other duties as assigned by the Board of Directors.

### 2.4 Risk Management Committee

The Risk Management Committee must be appointed by the Board of Directors and consist of at least three members, including at least one Company director. Each Risk Management Committee member may hold risk management directorships in no more than five listed companies, performing the following duties:

1. Consider and propose risk management policies related to the Company's business operations, acceptable risk criteria, and other relevant frameworks to the Board of Directors.
2. Develop enterprise-wide risk management systems for efficiency and continuously promote cooperation in risk management at all levels.
3. Review risk reports from various departments and provide recommendations and corrective guidelines.
4. Coordinate with the Audit Committee regarding significant risks and appropriate management measures.
5. Oversee the effectiveness of risk management processes.
6. Report risks and risk management results to Board of Directors' meetings according to the established schedule.
7. Perform other risk management tasks as assigned by the Board of Directors.

### 2.5 Corporate Governance Committee

The Corporate Governance Committee must be appointed by the Board of Directors and comprise at least three directors, with not less than half being independent directors, and the Chairman of the Corporate Governance Committee must be an independent director. Corporate Governance Committee members who retire by rotation may be reappointed as necessary and appropriate, performing the following duties:

1. Prepare corporate governance policies, business ethics and code of conduct, anti-corruption policies to comply with laws and regulations of government agencies and organizations overseeing the Company, such as the Stock Exchange of Thailand (SET) and the Securities and Exchange Commission (SEC), for presentation to the Board of Directors for consideration and approval.
2. Propose corporate governance guidelines, anti-fraud practices, ethics, and business code of conduct to the Board of Directors, as well as provide advice and recommendations to the Board of Directors on matters concerning corporate governance and anti-fraud practices, ethics, and business code of conduct.
3. Oversee the work performance of employees, executives, and the Board of Directors to comply with corporate governance policies, anti-corruption policies, ethics, and business code of conduct, as well as review and evaluate compliance with corporate governance policies together with directors and management, and provide recommendations regarding implementation of such policies.
4. Review corporate governance policies, business ethics and code of conduct, anti-corruption policies, and related practices to keep them current on an ongoing basis at least once per year, referencing laws, international best practices, and regulations of government agencies and organizations overseeing the Company, such as the Stock Exchange of Thailand (SET) and the Securities and Exchange Commission (SEC), for presentation to the Board of Directors for consideration and approval of improvements.
5. Report performance results, evaluation results of compliance with corporate governance policies, anti-corruption policies, and important issues concerning corporate governance and anti-fraud efforts to the Board of Directors at least once per year.
6. Oversee and monitor the progress of performance of various subcommittees established by the Corporate Governance Committee (if any), as well as provide necessary recommendations and support.
7. Coordinate with other sub-committees and various working groups in considering matters related to corporate governance and anti-fraud efforts, and provide advice as necessary.
8. Promote Company communications to ensure directors, executives, employees at all levels, and relevant parties are aware of and understand corporate governance policies and practices, ethics, business code of conduct, anti-corruption policies, and related practices adequately and continuously.
9. Perform other duties as the Board of Directors deems appropriate and assigns.

### 2.6 Sustainable Development Committee

The Sustainable Development Committee must be appointed by the Board of Directors and comprise at least three directors with at least one independent director. The Sustainable Development Committee shall select a committee member to serve as Chairman of the Sustainable Development Committee, whereby the Chairman must be an independent director (and must not hold the position of Chairman of the Board of Directors) to enable independent expression of opinions and performance of duties, performing the following duties:

1. Consider, establish, and review policies, strategies, operational frameworks, and improve the Company's sustainable development goals in compliance with laws, regulations, requirements, and in accordance with principles, good practices, and nationally and internationally accepted sustainability standards, comprehensively and with balance across environmental, social, and governance dimensions.
2. Provide advice to the Board of Directors and management, and promote the establishment of principles, policies, and strategies, including the Company's operational framework, to align with sustainable development principles according to established goals.
3. Support the Board of Directors, executives, and employees in conducting themselves according to the Company's sustainable development guidelines continuously and efficiently to establish an organizational culture.
4. Supervise and monitor sustainable development operations to comply with established policies, strategies, and goals efficiently.
5. Consider and approve guidelines for disclosing the Company's sustainable development operations to comply with practice criteria or disclosure standards at both national and international levels, with balance and efficiency, and maximum benefit to the Company and stakeholders.
6. Consider and approve sustainability reports and related reports for presentation to the Board of Directors for approval before public disclosure.
7. Evaluate the performance of the Sustainable Development Committee and report evaluation results to the Board of Directors.
8. Promote awareness among internal and external stakeholders and support cooperation with relevant stakeholders to drive sustainable development for broad effectiveness.
9. Stimulate and promote participation in sustainability assessments or rankings by nationally and internationally recognized organizations to continuously develop and elevate the Company's operational standards.
10. Monitor trends and sustainability situations that may impact the Company's operations continuously, making recommendations to the Board of Directors or relevant management, and consider and analyze and assess the Company's material sustainability issues.
11. Consider, review, and provide recommendations for improving the Sustainable Development Committee Charter to ensure it remains appropriate and current, and present to the Board of Directors for approval if changes occur.
12. Be responsible for any other matters assigned by the Board of Directors.

## 3. Independent Directors and Qualifications of Independent Directors

There must be at least three independent directors, comprising not less than one-third of the entire Board of Directors. They must be independent from major shareholders or groups of major shareholders and the Company's executives, have adequate access to the Company's financial and business information, including other businesses, to express opinions freely in protecting the interests of minority shareholders, regularly attend Board of Directors' meetings, and have the duty to prepare reports certifying their independence upon appointment and disclose independence information in the Company's annual report. Independent directors must possess complete qualifications as prescribed by the Stock Exchange of Thailand (SET) and the Securities and Exchange Commission (SEC), namely:

Qualifications of Independent Directors

Individuals who possess knowledge, capability, and qualifications consistent with the minimum criteria of the Securities and Exchange Commission and the requirements of the Stock Exchange of Thailand, as follows:

1. Hold not more than 1% of shares with voting rights.
2. Must not be a director participating in management, employee, staff member, salaried consultant, or person with controlling power within the two years prior. Relaxation applies in cases where the person has ceased being a government official or consultant to a government agency that is a major shareholder or person with controlling power for less than two years.
3. Must not be a person with blood relations or legal registration relationships with directors or executives.
4. Must not conduct transactions or be a significant shareholder or person with controlling power of a legal entity conducting transactions with the Company with a transaction value ≥ 20 million baht or 3% of NTA, whichever is lower, within the two years prior.
5. Must not be an auditor of the Company, parent company, subsidiaries, associated companies, major shareholders, or persons with controlling power within the two years prior.
6. Must not be a provider of other professional services or be a significant shareholder, person with controlling power, or partner of a legal entity providing services exceeding 2 million baht within the two years prior.

   In cases where individuals do not meet criteria 4 and 6, they may hold the position of independent director only if the Board of Directors demonstrates that it has considered according to Section 89/7 principles that there is no impact on performing duties and providing independent opinions, and must disclose the prescribed information in the shareholder meeting notice.
7. Must not be a representative of Company directors, major shareholders, or persons related to major shareholders.

8. Must not operate a business of the same nature and in competition with the Company and subsidiaries, or hold more than 1% of shares, or be a director participating in management, employee, staff member, salaried consultant, or person with controlling power in such business.

9. Must not have other characteristics that prevent the provision of independent opinions.

10. Independent directors may be independent directors of companies within the group, but Audit Committee members must not be directors of the parent company, subsidiaries, or sister companies (sibling companies) that are listed companies.

11. After being appointed as an independent director, such independent director may be delegated by the Board of Directors to make decisions regarding the Company's operations, parent company, subsidiaries, associated companies, sister companies, major shareholders, or persons with controlling power through collective decision-making, but Audit Committee members must not participate in operational decision-making.

In cases where a person appointed by the Company to hold the position of independent director is a person who has or has had business relationships or professional services exceeding the value specified in paragraph one, the Company shall be granted an exemption from the prohibition on having or having had (4) or (6), or professional service providers having had business relationships or professional services exceeding such value, only when the Company has arranged for the Board of Directors' opinion demonstrating that it has considered according to Section 89/7 principles that the appointment of such person has no impact on performing duties and providing independent opinions, and has arranged to disclose the following information in the shareholder meeting notice for the agenda item considering the appointment of independent directors:

(1) The nature of business relationships or professional services that cause such person to not meet the prescribed qualifications.
(2) Reasons and necessity for retaining or appointing such person as an independent director.
(3) The Board of Directors' opinion in proposing the appointment of such person as an independent director.

For the purposes of paragraph one (5) and (6), the term "partner" means a person assigned by an audit firm or professional service provider to sign the audit report or professional service report (as the case may be) on behalf of such legal entity. To promote opportunities for independent directors to meet and consult among themselves independently to provide recommendations and determine guidelines for developing good corporate governance quality, the Company has therefore scheduled independent director meetings at least twice per year.

## 4. Powers, Duties, and Responsibilities of the Board of Directors

According to the Company's regulations, the Board of Directors has the power and duty to conduct the Company's business in accordance with laws, objectives, regulations, and resolutions of shareholder meetings by adhering to the principles of "Code of Best Practices for Directors of Listed Companies" as prescribed by the Stock Exchange of Thailand, with honesty and prudence in safeguarding the Company's interests and for the maximum benefit of shareholders. Therefore, the Company has established the roles, duties, and practices of the Board of Directors to serve as a model for employees at all levels to follow as guidelines for performing their work and to build confidence among shareholders and investors in general, as follows:

1. Oversee and manage the Company's operations and performance of duties in accordance with laws, objectives, the Company's regulations, and shareholder meeting resolutions with integrity (Duty of Loyalty), anti-fraud and anti-corruption (Anti-Corruption), prudence (Duty of Care), accountability (Duty of Accountability), and ethics (Ethics), safeguarding the Company's best interests based on good corporate governance principles, while considering the interests of all shareholders equitably.
2. Establish the business vision, consider and approve important policies and strategies, financial objectives, various plans, budgets, and risks, as well as supervise and control management to implement operations according to established policies and plans efficiently and effectively, and be accountable for operating results and executive performance with diligence and prudence in work performance.
3. Ensure that the accounting system, financial reporting, and auditing are reliable, including overseeing the establishment of processes for assessing the appropriateness of internal controls and internal auditing for efficient and effective financial reporting and monitoring. The Board of Directors has prepared a report on the Board of Directors' responsibility for financial reports displayed alongside the auditor's report in the annual report.
4. Monitor and manage the resolution of conflicts of interest that may arise among the Company's stakeholders, establish guidelines for conducting transactions that may have conflicts of interest, primarily for the benefit of the Company and shareholders as a whole, whereby stakeholders should not participate in decision-making, establishing procedures for implementation and complete and accurate disclosure of information regarding transactions that may have conflicts of interest.
5. Establish a Risk Management Policy covering the entire organization, with management implementing the policy and reporting risk management results to the Board of Directors through quarterly reports via the Audit Committee. The Company arranges for risk management effectiveness evaluations at least once per year, emphasizing early warning signals and various irregularities.

6. Consider appointing individuals who possess qualifications and do not have prohibited characteristics as specified in the Public Limited Companies Act B.E. 2535 and laws governing securities and stock exchanges, including related notifications, regulations, and/or rules to hold directorship positions in cases where director positions become vacant for reasons other than retirement by rotation.

7. Consider appointing independent directors by considering the qualifications and prohibited characteristics of independent directors according to laws governing securities and stock exchanges, notifications of the Capital Market Supervisory Board, including related notifications, regulations, and/or rules of the Stock Exchange of Thailand, or propose to the shareholder meeting for consideration to appoint as the Company's independent directors.

8. Consider appointing the Audit Committee with qualifications as required by laws governing securities and stock exchanges, notifications of the Capital Market Supervisory Board, including notifications, regulations, and/or rules of the Stock Exchange of Thailand.

9. Consider appointing the Executive Committee and delegate certain powers and duties to the Executive Committee to manage the Company's operations. Executive directors are entitled to receive remuneration and bonuses as determined by the Board of Directors' meeting; however, this does not affect the rights of such executive directors to receive remuneration or benefits under the Company's regulations in their capacity as directors, employees, or staff of the Company.

10. Promote the establishment of written business ethics to ensure all directors, executives, and employees understand the ethical standards the Company uses in conducting business, whereby the Board of Directors will monitor strict compliance with such ethics.

11. Appoint a Company Secretary in accordance with laws governing securities and stock exchanges to perform duties of preparing and maintaining documents and other matters as prescribed by the Capital Market Supervisory Board, and assist in various activities of the Board of Directors and the Company, including Board of Directors' meetings and shareholder meetings, as well as providing advice to directors and the Company on proper conduct and business operations in accordance with laws and related regulations consistently, and ensuring that directors and the Company disclose information accurately, completely, and transparently.

12. Establish an Anti-Corruption Policy covering the entire organization.

13. The Company Secretary summarizes reports on securities holdings of themselves, their spouses, and minor children holding shares in the Company and affiliated companies at Board of Directors' meetings. Directors must promptly notify the Company through the Company Secretary when the following occurs:

- Having direct or indirect interests in any contract that the Company enters into during the accounting year
- Changes in shareholding proportions in the Company and affiliated companies

14. Attend at least one course from the Thai Institute of Directors (IOD) related to directorship, namely the Director Accreditation Program (DAP) or Director Certification Program (DCP) or equivalent to enhance skills and capabilities in performing duties.
15. Other duties of directors as specified in notifications, requirements, acts, or any other laws governing the Company.
16. Evaluate compliance with the Company's good corporate governance policy and conduct regular reviews.
17. The Board of Directors has the authority to establish and amend the names of directors who have the authority to sign and bind the Company.
18. The Board of Directors has the duty to verify and certify the Company's financial statements to be accurate in accordance with laws, transparent accounting standards.

## 5. Powers, Duties, and Responsibilities of the Audit Committee

1. Review financial reports to ensure accuracy and reliability, including adequate disclosure, by coordinating with certified public accountants and executives responsible for preparing both quarterly and annual financial reports.
2. Review to ensure the Company and affiliated companies have appropriate and effective internal control systems, internal audit systems, and risk management systems, and may recommend reviews or audits of any matters deemed necessary and important, as well as provide recommendations regarding improvements to internal control systems and risk management systems, and report review results to the Board of Directors.
3. Review the Company's compliance with laws governing securities and stock exchanges or requirements of the Stock Exchange of Thailand, policies, rules, regulations, and other laws related to the Company.
4. Review evidence if there are doubts regarding operations that may have a material impact on the Company's financial position and operating results, or conflicts of interest, or violations of laws and related requirements that may affect the Company's operations.
5. Consider the Company's information disclosure in cases of connected transactions or transactions that may have conflicts of interest to ensure compliance with laws and Stock Exchange requirements, to ensure such transactions are reasonable and most beneficial to the Company.

6. Consider selecting and proposing the appointment of independent individuals to serve as the Company's certified public accountants, including considering proposing auditor remuneration by taking into account the credibility, adequacy of resources and audit workload of that audit firm, including the experience of audit firm personnel assigned to audit the Company's accounts, as well as meeting with certified public accountants without management present at least once per year.
7. Review the accuracy and effectiveness of information technology related to financial reporting and internal controls.
8. Promote the development of financial reporting systems to be comparable with international accounting standards.
9. Review the Company's internal audit work plans according to generally accepted methods and standards.
10. Consider the independence of the internal audit department or engagement of external parties as internal auditors, including providing advice on the budget and personnel of the internal audit department, as well as approving the consideration of appointment, transfer, and termination of the head of the internal audit department and evaluating the annual performance of the head of the internal audit department.
11. Prepare the Audit Committee's report, signed by the Chairman of the Audit Committee and disclosed in the Company's annual report in accordance with the criteria prescribed by the Stock Exchange of Thailand.
12. The Audit Committee may seek independent opinions from any other professional advisors when deemed necessary at the Company's expense with the approval of the Board of Directors, whereby engagement shall be in accordance with the Company's regulations and requirements.
13. The Chairman of the Audit Committee or Audit Committee members must attend the Company's shareholder meetings to provide clarification on matters concerning the Audit Committee or the appointment of auditors.
14. Consider reviewing and updating the Audit Committee Charter.
15. Perform other duties as assigned by the Board of Directors with the approval of the Audit Committee.
16. Review the "Self-Assessment Form on Anti-Corruption Measures" by reviewing the appropriateness of compliance with the self-assessment form on anti-corruption measures and ensuring the information in this self-assessment form is accurate and sufficient for submission to the Thai Private Sector Collective Action Against Corruption for the purpose of entering the Certification Process.

## 6. Powers, Duties, and Responsibilities of the Nomination and Remuneration Committee

The Nomination and Remuneration Committee has duties and responsibilities as assigned by the Board of Directors to undertake the following matters:

1. Establish appropriate qualifications, policies, criteria, and methods for nominating Company directors and the Chief Executive Officer, as well as conduct recruitment and selection of individuals possessing qualifications in accordance with prescribed regulations and relevant laws, then present to the Board of Directors and/or shareholder meeting for approval (as applicable) for consideration to hold positions as directors and Chief Executive Officer.
2. Establish policies, criteria, and methods for determining both monetary and non-monetary remuneration for the Board of Directors and sub-committees appropriate to their duties and responsibilities, consistent with the Company's operating results and market conditions, to seek approval from the Board of Directors and request approval from the shareholder meeting.
3. Determine necessary and appropriate remuneration, both monetary and non-monetary, to motivate and retain the Board of Directors, sub-committees, and Chief Executive Officer.
4. Ensure the Board of Directors has an appropriate composition consistent with the changing environment and circumstances, whereby the Board of Directors must comprise individuals with knowledge, capability, and experience in various fields.
5. Establish guidelines and evaluate the performance of directors and the Chief Executive Officer to consider annual remuneration adjustments, taking into account duties, responsibilities, and related risks, as well as emphasizing the enhancement of long-term shareholder value as part of the performance evaluation.
6. Disclose policies and details of the nomination process, remuneration determination policies, and disclose remuneration in various forms, as well as prepare remuneration determination reports, which must include at least details regarding objectives, operations, and opinions of the Nomination and Remuneration Committee in the Company's annual report.
7. Review the charter of the Nomination and Remuneration Committee annually. In cases where the Committee deems it necessary to modify the content of such charter to be appropriate with regulations, requirements, and changing circumstances, the Nomination and Remuneration Committee shall propose to the Board of Directors for consideration of changes.
8. Plan and prepare succession plans for the Company's executives and propose to the Board of Directors for approval to ensure planning and preparation of personnel in positions critical to business operations.
9. Appoint or seek advice from independent external advisors when necessary, with the Company bearing the expenses.
10. Perform other duties as assigned by the Board of Directors.

## 7. Powers, Duties, and Responsibilities of the Executive Committee

1. Be responsible for managing matters concerning ordinary business operations and administrative work of the Company, considering and establishing policies, direction, and strategies for the Company's business operations, determining financial plans, budgets, human resource management, information technology investments, and the Company's public relations, for presentation to the Board of Directors' meeting for approval and/or endorsement, including monitoring and following up on the Company's operating results according to established policies.
2. Conduct and manage the Company's affairs in accordance with objectives, regulations, policies, rules, requirements, orders, and resolutions of the Board of Directors' meetings and/or shareholder meetings of the Company in all respects.
3. Have the authority to appoint and supervise the operations of appointed working groups to achieve established policies and goals.
4. Have the authority to approve financial expenditures in capital expenditures (per transaction) not exceeding 10 million baht, whereby such matters must be presented to the Board of Directors' meeting for approval/ratification.
5. Approve significant investment expenditures specified in the annual expenditure budget as assigned by the Board of Directors or as previously approved in principle by resolution of the Board of Directors.
6. Have the authority to approve short-term investments (not exceeding one year) and portfolio investments with a term of 2-5 years for the Company in amounts (per transaction) not exceeding 300 million baht, whereby such matters must be presented to the Board of Directors' meeting for ratification.
7. Consider proposing interim dividends or annual dividends to the Board of Directors for consideration and approval.
8. Establish organizational structure, organizational management authority, including appointment, employment, transfer, determination of salaries, remuneration, and bonuses for executive-level employees who do not hold positions as executive directors, and termination.

The authority of the Executive Committee shall not include approval of any transaction that may have conflicts of interest or any transaction in which the Executive Committee or persons who may have conflicts have interests or benefits of any other nature that conflict with the Company or subsidiaries according to the regulations of the Securities and Exchange Commission and the Stock Exchange of Thailand, whereby approval of such transactions must be presented to the Board of Directors' meeting and/or shareholder meeting for consideration and approval of such transactions as required by the Company's regulations or relevant laws.

## 8. Powers, Duties, and Responsibilities of the Corporate Governance Committee

The Corporate Governance Committee has the authority to undertake various actions within the scope of responsibilities specified in the duties and responsibilities section, and has the authority to undertake the following:

1. Have the authority to invite management or relevant parties or appropriate persons to attend meetings or request clarification or information on related matters as necessary.
2. Have the authority to engage consultants or independent external persons or professional experts to provide opinions or advice as necessary.
3. Have the authority to appoint and define the roles, duties, and responsibilities of subcommittees or working groups to assist in corporate governance as necessary, and have the authority to direct and supervise the operations of such subcommittees or working groups to ensure the Company has an effective corporate governance framework consistent with the changing business environment, technology, and risks.
4. Prepare corporate governance policies, business ethics and code of conduct, anti-fraud and anti-corruption policies to comply with laws and regulations of government agencies and organizations overseeing the Company, such as the Stock Exchange of Thailand (SET) and the Securities and Exchange Commission (SEC), for presentation to the Board of Directors for consideration and approval.
5. Propose corporate governance guidelines, anti-fraud practices, ethics, and business code of conduct to the Board of Directors, as well as provide advice and recommendations to the Board of Directors on matters concerning corporate governance and anti-fraud practices, ethics, and business code of conduct.
6. Oversee the work performance of employees, executives, and the Board of Directors to comply with corporate governance policies, anti-fraud and anti-corruption policies, ethics, and business code of conduct, as well as review and evaluate compliance with corporate governance policies together with directors and management, and provide recommendations regarding implementation of such policies.
7. Review corporate governance policies, business ethics and code of conduct, anti-fraud and anti-corruption policies, and related practices to keep them current on an ongoing basis at least once per year, referencing laws, international best practices, and regulations of government agencies and organizations overseeing the Company, such as the Stock Exchange of Thailand (SET) and the Securities and Exchange Commission (SEC), for presentation to the Board of Directors for consideration and approval of improvements.
8. Report performance results, evaluation results of compliance with corporate governance policies, anti-fraud and anti-corruption policies, and important issues concerning corporate governance and anti-fraud efforts to the Board of Directors at least once per year.
9. Oversee and monitor the progress of performance of various subcommittees established by the Corporate Governance Committee (if any), as well as provide necessary recommendations and support.

10. Coordinate with other sub-committees and various working groups in considering matters related to corporate governance and anti-fraud efforts, and provide advice as necessary.
11. Promote Company communications to ensure directors, executives, employees at all levels, and relevant parties are aware of and understand corporate governance policies and practices, ethics, business code of conduct, anti-fraud and anti-corruption policies, and related practices adequately and continuously.
12. Perform other duties as the Board of Directors deems appropriate and assigns.
13. Hold meetings at least twice per year, and at every meeting, at least one independent director must attend.
14. Conduct self-performance evaluations and report results to the Board of Directors for acknowledgment once per year.
15. Report the performance results of the Corporate Governance Committee to the Board of Directors for acknowledgment at least twice per year, and prepare a report of the Corporate Governance Committee for disclosure in the Company's annual report.

## 9. Powers, Duties, and Responsibilities of the Sustainable Development Committee

1. Consider, establish, and review policies, strategies, operational frameworks, and improve the Company's sustainable development goals in compliance with laws, regulations, requirements, and in accordance with principles, good practices, and nationally and internationally accepted sustainability standards, comprehensively and with balance across environmental, social, and governance dimensions.
2. Provide advice to the Board of Directors and management, and promote the establishment of principles, policies, and strategies, including the Company's operational framework, to align with sustainable development principles according to established goals.
3. Support the Board of Directors, executives, and employees in conducting themselves according to the Company's sustainable development guidelines continuously and efficiently to establish an organizational culture.
4. Supervise and monitor sustainable development operations to comply with established policies, strategies, and goals efficiently.
5. Consider and approve guidelines for disclosing the Company's sustainable development operations to comply with practice criteria or disclosure standards at both national and international levels, with balance and efficiency, and maximum benefit to the Company and stakeholders.
6. Consider and approve sustainability reports and related reports for presentation to the Board of Directors for approval before public disclosure.
7. Evaluate the performance of the Sustainable Development Committee and report evaluation results to the Board

of Directors at least three times per year.

8. Promote awareness among internal and external stakeholders and support cooperation with relevant stakeholders to drive sustainable development for broad effectiveness.
9. Stimulate and promote participation in sustainability assessments or rankings by nationally and internationally recognized organizations to continuously develop and elevate the Company's operational standards.
10. Monitor trends and sustainability situations that may impact the Company's operations continuously, making recommendations to the Board of Directors or relevant management, and consider and arrange for analysis and assessment of the Company's material sustainability issues.
11. Consider, review, and provide recommendations for improving the Sustainable Development Committee Charter to ensure it remains appropriate and current, and present to the Board of Directors for approval if changes occur. Be responsible for any other matters assigned by the Board of Directors.
12. Hold meetings as the Sustainable Development Committee or the Chairman of the Committee deems appropriate, with meetings held at least three times per year or in special cases as deemed appropriate.
13. Prepare the Sustainable Development Committee report for disclosure in the Company's annual report, signed by the Chairman of the Sustainable Development Committee.
14. Conduct self-performance evaluations and report problems and challenges that may contribute to not achieving sustainability objectives or indicators to the Board of Directors at least once per year.

## 10. Powers, Duties, and Responsibilities of the Risk Management Committee

The Risk Management Committee has duties and responsibilities covering the following matters:

1. Establish risk management policies, objectives, and strategies.
2. Develop enterprise-wide risk management systems for efficiency and continuously promote cooperation in risk management at all levels.
3. Monitor and review risks of various departments and provide recommendations and corrective guidelines.
4. Oversee the effectiveness of risk management processes.
5. Report risks and risk management results to Board of Directors' meetings according to the established schedule.
6. Appoint sub-working groups and supervise the appointed working groups to perform their assigned duties.
7. Review risk management policies and related manuals and documents at least once per year, reporting the appropriateness and effectiveness of implementation to the Board of Directors.

## 11. Role, Duties, and Responsibilities of the Company Secretary

The Company Secretary plays an important role in the Company's corporate governance, with strategic and supervisory roles to support the work of the Board of Directors, as well as ensuring the Company operates in accordance with laws, regulations, and good corporate governance principles, with details as follows:

1. Provide advice to the Board of Directors regarding laws, rules, the Company's various regulations, and related practices, as well as monitor proper and consistent compliance.
2. Oversee and support the work of the Board of Directors to proceed smoothly and efficiently in accordance with the Public Limited Companies Act B.E. 2535, securities laws, and related laws.
3. Prepare and maintain the Company's important documents, such as the register of directors, notices of Annual General Meetings and Board of Directors' meetings, minutes of Annual General Meetings and Board of Directors' meetings, annual reports, and reports of interests reported by directors or executives.
4. Perform duties in organizing Annual General Meetings and Board of Directors' meetings.
5. Prepare important information reports for submission to the Stock Exchange of Thailand and regulatory agencies, accurately and completely in accordance with laws, in both Thai and English.
6. Contact, communicate with, and appropriately care for shareholders to ensure shareholders are informed of their various rights and the Company's news.
7. Coordinate with regulatory agencies such as the Stock Exchange of Thailand, the Securities and Exchange Commission, and the Ministry of Commerce.
8. Ensure the Company Secretary's office serves as the central repository for organizational information, such as the juristic person registration certificate, memorandum of association, articles of association, shareholder register, and various important legal documents.
9. Arrange orientation and provide advice to newly appointed directors.

## 12. Board of Directors' Meetings

Board of Directors' meetings shall be scheduled in advance each year to enable directors to arrange their time and attend meetings, with the Chairman of the Board of Directors approving the inclusion of meeting agenda items by consulting with the Chief Executive Officer, as well as considering requests from directors to include other important matters as agenda items for each meeting. The Company shall send meeting documents to directors for advance consideration to allow sufficient time to study, consider, and make proper decisions on various matters, with the following practices:

1. The Company's regulations require the Board of Directors to meet at least once every three months and hold shareholder meetings at least once per year, whereby at least half of the Company directors must be present to constitute a quorum.
2. The Company arranges to send meeting notices to directors for consideration at least seven days before the meeting date to allow directors sufficient time to study, consider, and make proper decisions on various matters, and arrange time to attend meetings.
3. The Chairman of the Board of Directors approves the arrangement of matters to be included on the Board of Directors' meeting agenda by consulting with the Chief Executive Officer and considering requests from directors to include other important matters as agenda items for the next meeting.
4. The Chairman of the Board of Directors should allocate sufficient time for management's presentation of documents and information, and for the Board of Directors' consideration, inquiry, and discussion of important issues.
5. The Board of Directors must dedicate time and devote full attention to the Company and be ready to attend meetings regularly.
6. The Board of Directors can access necessary information to request documents, information, advice, and various services regarding the Company's operations from senior management, and may request independent opinions from external advisors when necessary for each meeting.
7. The Board of Directors may invite senior management to attend Board of Directors' meetings to provide additional detailed information on relevant matters.
8. Company directors who may be involved or have interests in any meeting agenda item must abstain from voting or providing opinions on that agenda item.
9. The number of Board of Directors' meetings should be determined appropriately according to the duties and responsibilities of the Board of Directors and the nature of the Company's business operations.
10. Minutes of Board of Directors' meetings, meeting results, and opinions of the Board of Directors must be clear for reference purposes.
11. On average, each Company director should attend no less than 80% of all meetings throughout the year.
12. All Company directors should attend at least 75% of meetings throughout the year.
13. The Board of Directors has established a policy regarding the minimum quorum at the time the Board of Directors votes at Board of Directors' meetings, requiring the presence of no less than two-thirds of all Company directors. In cases of voting by directors without interests only, there must be no less than two-thirds of Company directors without interests present.
14. Arrange meetings among non-executive directors without management participation once per year.

## 13. Appointment and Removal of Company Directors

### 1. Criteria for Nomination and Appointment of Directors

In appointing the Board of Directors, the Nomination and Remuneration Committee is responsible for considering, selecting, and screening individuals with appropriate qualifications according to the Company's regulations and without prohibited characteristics as specified in relevant laws and regulations, whereby independent directors must possess complete qualifications according to the notifications of the Capital Market Supervisory Board and shall propose the names of individuals with such appropriate qualifications to the Board of Directors for approval to present such director names to the Annual General Meeting for election of directors according to the following criteria. The Nomination and Remuneration Committee has considered the nature of business operations and future direction, whereby candidates must possess knowledge, business experience, or relevant industry experience, as well as using tools to assist in considering qualifications or skills necessary for the Board of Directors (Board Skill Matrix), which has been prepared for the Company.

The Board of Directors shall comprise no fewer than five directors, with not less than half of all directors residing in the Kingdom of Thailand and possessing qualifications as required by law. The nomination of Company directors and consideration of Company director qualifications shall be in accordance with the following criteria:

1) The appointment of Company directors shall be in accordance with the Company's regulations and requirements of relevant laws, with transparency and clarity, whereby consideration must include the individual's educational background and professional experience, including knowledge and business capabilities relevant to the Company, with sufficient details to benefit the decision-making of the Board of Directors and shareholders. Company directors must be individuals with knowledge and capability, transparency, honesty, integrity, virtue, ethics in conducting business, and sufficient time to dedicate their knowledge, capabilities, and perform duties for the Company.
2) Directors are prohibited from operating businesses, entering into partnerships, or serving as directors in other legal entities of the same nature and in competition with the Company's business, unless disclosed to the shareholder meeting before the appointment resolution, and directors must promptly notify the Company if they have interests in contracts made by the Company or hold shares or debentures that increase or decrease in the Company or subsidiaries or affiliated companies.
3) Must possess qualifications and not have prohibited characteristics under the Public Limited Companies Act and laws governing securities and stock exchanges.

The shareholder meeting shall elect directors according to the following criteria and methods:

1) Each shareholder shall have votes equal to one (1) share per one (1) vote.
2) Each shareholder may use all votes under 1. to elect one or more persons as directors, but may not allocate votes to any person in greater or lesser amounts.

3) Persons receiving the highest votes in descending order shall be elected as directors equal to the number of directors to be appointed or elected at that time. In cases where persons elected in the next order receive equal votes exceeding the number of directors to be appointed, the Chairman of the meeting shall cast the deciding vote.

### 2. Removal and Termination of Directors

1) At every Annual General Meeting, one-third (1/3) of directors at that time shall retire from office. If the number of directors cannot be divided exactly into three parts, the number closest to one-third (1/3) shall retire, and retiring directors may be re-elected to office. Directors required to retire in the first and second years following the Company's conversion registration shall be determined by drawing lots, while in subsequent years, directors who have served the longest shall retire.
2) In addition to retirement by rotation, directors shall vacate office upon death, resignation, lack of qualifications, or having prohibited characteristics under the Public Limited Companies Act and/or laws governing securities and stock exchanges, or by shareholder meeting resolution for removal, or by court order for removal.
3) Any director wishing to resign from office shall submit a resignation letter to the Company, whereby the resignation shall take effect from the date the resignation letter reaches the Company. The resigning director may also notify the Registrar of their resignation.
4) In voting to remove any director from office before retirement by rotation, votes of not less than three-quarters (3/4) of shareholders attending the meeting and entitled to vote, holding shares totaling not less than half of the shares held by shareholders attending the meeting and entitled to vote, shall be required.
5) In cases where a director position becomes vacant for reasons other than retirement by rotation, the Board of Directors shall elect a person possessing qualifications and without prohibited characteristics under the Public Limited Companies Act and laws governing securities and stock exchanges as a replacement director at the next Board of Directors' meeting, unless the remaining term of that director is less than two (2) months, whereby the person entering as a replacement director shall serve only the remaining term of the director they replace.
6) Board of Directors' resolutions must comprise votes of not less than three-quarters (3/4) of the remaining directors.

## 14. Performance Evaluation of the Board of Directors

### 1. Performance Evaluation of the Board of Directors and Sub-Committees

The Nomination and Remuneration Committee has considered the IOD's self-assessment guidelines to arrange for the Board of Directors and sub-committees to conduct regular performance evaluations at least once per year, with the following topics for evaluating the performance of the Board of Directors as a whole:

i. Structure and qualifications of the Board of Directors
ii. Roles, duties, and responsibilities of the Board of Directors
iii. Board of Directors' meetings
iv. Dynamics in the performance of the Board of Directors' duties
v. Relationship with management
vi. Director development
vii. Board of Directors' reporting (for sub-committees)

For individual director performance evaluations, the topics are as follows:

i. Personal qualifications
ii. Readiness to perform duties
iii. Participation in meetings
iv. Roles, duties, and responsibilities
v. Relationships with the Board of Directors and management

The evaluation process comprises the following steps:

1. The Company Secretary distributes such evaluation forms to each director to conduct evaluations in both collective and individual formats.
2. The Company Secretary compiles and presents to the Nomination and Remuneration Committee.
3. The Nomination and Remuneration Committee summarizes the results to present approaches for improving efficiency and operations to the Board of Directors for maximum benefit to the Company's stakeholders and in accordance with good corporate governance principles.

### 2. Performance Evaluation of Senior Management

The Nomination and Remuneration Committee has established guidelines for evaluating the performance of senior management (C-Level and executives reporting directly to the Managing Director), including the Managing Director, Deputy Managing Director, Chief Executive Officer, Senior Directors, and Chief Officers in various departments, using the tool OKR (Objectives and Key Results) with the following evaluation criteria:

1) Senior management establishes their own quarterly goals and key performance indicators, which must align with the Company's vision, goals, and objectives.
2) Individual goals and key performance indicators will be considered and reviewed, including receiving additional recommendations from the Nomination and Remuneration Committee to ensure that all senior management's goals and operational plans comprehensively cover important issues, including financial performance goals, business expansion goals, quality development goals, sustainable business operation goals, and the ability to drive the organization efficiently and effectively.

The steps for performance evaluation using OKR are as follows:

1. At the beginning of each quarter, senior management prepares individual goals and key performance indicators for presentation to the Nomination and Remuneration Committee, whereby the Nomination and Remuneration Committee, together with supervisors in the reporting line, considers the presentations and provides recommendations or adds goals and key performance indicators to comprehensively cover important issues and align with the Company's context.
2. The Secretary of the Nomination and Remuneration Committee compiles the OKRs of all senior management that have been presented and revised according to recommendations.
3. The Nomination and Remuneration Committee requires senior management to report quarterly on performance results according to such individual goals and key performance indicators to summarize results and present to the Board of Directors to discuss challenges and review relevant strategies.
4. Such performance evaluation results will be used to consider the appropriateness of remuneration, determine annual remuneration adjustment rates, and annual bonus payment rates.

## 15. Recruitment and Appointment of Senior Management

For the recruitment of senior management, the Board of Directors has assigned the Managing Director to be responsible for recruiting senior management, whereby the Nomination and Remuneration Committee shall review whether the recruited senior management possesses complete and appropriate qualifications, knowledge, capabilities, experience, including skills and attitudes that are beneficial to the Company's operations, to help drive the organization's operations in accordance with the established direction and achieve the established goals.

## 16. Remuneration of Company Directors, Managing Director, and Chief Executive Officer

1. The Company has a policy to determine remuneration for Company directors, Managing Director, and Chief Executive Officer at a level that is attractive and comparable to companies in the same industry, whereby consideration shall be linked to the performance and responsibilities of directors, Managing Director, and Chief Executive Officer, as well as the Company's operating results. Each year, the Board of Directors, through the consideration and presentation of the Nomination and Remuneration Committee, shall consider and determine such remuneration and present it to the Annual General Meeting for approval.
2. Company directors assigned additional special duties and responsibilities shall receive additional remuneration linked to the level of responsibility assigned. The Chairman of the Board of Directors may receive additional remuneration beyond what Company directors receive.

3. The Board of Directors reviews reports regarding director remuneration payment policies, the principles, rationale, and objectives of policies prepared by the Nomination and Remuneration Committee, and discloses them in the Company's annual report and financial statements.
4. The Nomination and Remuneration Committee establishes evaluation criteria and evaluates the performance of senior management, including the Managing Director, Deputy Managing Director, Chief Executive Officer, Senior Directors, and Chief Officers of various departments, annually for use in determining senior management remuneration using the tool OKR (Objectives and Key Results). The above evaluation results will be presented to the Board of Directors for approval.
5. The Board of Directors has established a remuneration structure for non-executive Company directors divided into two parts. The first part is monetary remuneration, including monthly remuneration, meeting allowances, director bonuses, and other remuneration consisting of Directors and Officers Liability and Company Reimbursement Policy (D&O). The second part is non-monetary remuneration, including medical treatment benefits at hospitals affiliated with the Company.

## 17. Development of Directors and Executives

Knowledge and Understanding of Duties

1. When new directors are appointed, the Nomination and Remuneration Committee has assigned the Company Secretary to deliver the charter and corporate governance policy to newly appointed directors, as well as introduce the roles, duties, and responsibilities of directors, and coordinate to ensure directors receive orientation from management and receive documents including information about the Company, the nature of business operations, organizational mission, and business direction.
2. Additionally, the Nomination and Remuneration Committee has assigned the Company Secretary to inform directors of news about the opening of various courses relevant and necessary for performing Company director duties completely, comprehensively, transparently, in accordance with good corporate governance principles, and to best protect the interests of all stakeholders.
3. In cases where senior management is recruited and selected to join the Company, the Company will arrange in-depth orientation to ensure new senior management receives information about the Company, the nature of business operations, organizational mission, business direction, and receives presentations on the scope of work from various main departments to see an overview of organizational operations.

## Succession Planning

The Nomination and Remuneration Committee monitors and requires management to plan for the development and succession of senior management positions to ensure business continuity, whereby it will jointly recruit and screen qualifications to ensure personnel who will assume important positions in the Company possess appropriate qualifications, including educational credentials, experience, skills, and attitudes, and comply with relevant laws and regulatory requirements.

## Director Development

The Company has promoted and supported training and education on the Company's corporate governance principles for specialized committees to continuously enhance and develop performance. Additionally, all Company directors have completed the DCP course from the Thai Institute of Directors (IOD), as well as other courses related to their positions, such as Role of the Chairman Program (RCP), Advanced Audit Committee Program (AACP), Director Accreditation Program (DAP), Strategic Board Master Class, and Executive Development Program (EDP).

## Executive Development

The Company supports programs for developing executives and senior management annually by facilitating the search for external development courses and organizing internal development courses to enhance executives' knowledge in good corporate governance, sustainable business operations, and other skills, as well as stimulating the exchange and advancement of experiences among themselves, which will elevate potential and operational efficiency for the organization.

## Oversight of Compliance and Review

The Board of Directors shall ensure that Company directors, specialized committees, executives, and employees strictly comply with the best practices of the "Corporate Governance Policy" to continuously elevate and develop the quality of the Company's corporate governance, to create stability and sustainability for the organization, shareholders, and all stakeholder groups. The Board of Directors and Audit Committee require annual review of the "Corporate Governance Policy" manual.

# Ethics, Policies, and Practices Related to Corporate Governance

## Core Ethics that Executives Should Adhere to and Practice

To declare the intention to serve as a role model for employees in conducting themselves and performing work with honesty and integrity, as well as protecting the interests of all stakeholder groups equitably, management has selected core ethics to emphasize strict adherence by all executives, in addition to other ethics according to the "Corporate Governance Policy," with the important objective of promoting organizational values and culture that result in sustainable growth of the Company with virtue and compliance with laws, as follows:

1. Perform duties with responsibility, honesty, integrity, commitment, and dedication, comply with laws, rules, and the Company's policies, prioritizing the Company's interests.
2. Strictly maintain the confidentiality of customers, business partners, and the Company by carefully ensuring that documents or confidential information of the Company do not leak.
3. Respect the personal rights of other employees, not disclosing or criticizing information or stories about other employees, both personal and other matters, in a manner that would cause damage to employees or the overall image of the Company.
4. Do not slander or take any actions that lead to division or internal damage to the Company or persons associated with the Company.
5. Maintain and collaborate to create harmony among colleagues.
6. Treat colleagues with courtesy, kindness, good interpersonal relationships, and keep promises.
7. Conduct oneself and develop in ways that are beneficial to oneself and the Company according to organizational values.
8. Adhere to virtue and abstain from all vices, not conducting oneself in ways that may damage one's own reputation and the Company's reputation.
9. Pay attention to and assist in any actions that will maintain the work environment and atmosphere, including developing the organization toward excellence.
10. Avoid giving and/or receiving gifts, giving and/or receiving entertainment, or any benefits from business partners or persons involved in the Company's business, except for the benefit of conducting the Company's legitimate business or during festivals or customary occasions at appropriate values. If gifts received in the form of money or items have a value exceeding three thousand baht, refuse to accept and return them.

    In cases of giving gifts or souvenirs valued at no more than three thousand baht, or entertaining business partners or persons involved in the Company's business, it should be in accordance with normal business practice and custom.
11. Avoid behavior that constitutes sexual harassment.

## Ethics, Important Policies, and Other Practices Related to Corporate Governance Principles

The Company has established work ethics and business ethics to serve as guidelines for good business conduct for the Board of Directors, specialized committees, executives, and employees to adhere to, emphasizing the important principles of corporate governance, the importance of treating stakeholders equitably, fairly, and verifiably, complying with laws, and considering and respecting the rights of all stakeholder groups to create balance in society as a whole. The Company places importance on continuous personnel development in terms of knowledge and capabilities, virtue, and ethics by building a behavioral foundation focused on learning, diligently developing products and services, transferring knowledge to one another, and instilling a consciousness of honesty, integrity, perseverance, patience, and responsibility based on human dignity.

### 1) Ethics for the Board of Directors, Specialized Committees, Executives, and Employees

#### 1.1 Personal Conduct

1. Perform duties in accordance with laws related to business operations, objectives, the Company's regulations, corporate governance principles, and shareholder meeting resolutions.
2. Seek knowledge and experience to enhance oneself to become knowledgeable and capable in order to perform work more efficiently and effectively.
3. Adhere to virtue and must not seek positions, favors, or any other benefits improperly from supervisors or any other persons.
4. Abstain from all vices and addictive substances, not conducting oneself in ways that may damage one's own honor and reputation and the Company's reputation, such as not becoming heavily indebted, not being obsessed with all types of gambling, and not being involved with all types of addictive substances.
5. Not engage in occupations, professions, or actions that will affect the performance of duties or the reputation of oneself and the Company.
6. Avoid financial obligations with persons doing business with the Company or between employees themselves, which includes lending or borrowing money, various solicitations, share schemes, etc., except for charitable and public activities.
7. Not seek improper benefits, whether directly or indirectly.
8. Not take any actions that constitute managing or administering any other company that undermines the Company's interests or benefits any person or legal entity, whether for one's own benefit or others' benefit.
9. Maintain and collaborate to create harmony among colleagues.

## 1.2 Conduct Toward Colleagues

1. Enhance teamwork by cooperating and helping one another for the benefit of the Company's work as a whole.
2. Treat colleagues with courtesy, kindness, and good interpersonal relationships, adapt to work with others, and not conceal information necessary for colleagues' work performance.
3. Respect others by not falsely claiming others' work as one's own.
4. Supervisors should conduct themselves respectably and serve as good role models for subordinates, as well as being courteous to subordinate employees and colleagues at all levels.
5. Subordinates should treat supervisors with respect.
6. Subordinates should listen to supervisors' advice and not work over their immediate supervisors, except when ordered by higher supervisors, and be courteous to employees and colleagues at all levels.
7. Avoid disclosing or criticizing information or stories about other employees, both work-related and personal matters, in ways that would cause damage to employees or the Company's overall image.
8. Not engage in any immoral actions or sexual harassment toward other employees, whereby such actions cause distress, annoyance, or create a work environment that undermines morale, is hostile, or aggressive, including unreasonably interfering with other employees' work performance. Such behavior includes molestation, indecency, or sexual assault whether verbal or physical.

## 1.3 Conduct Toward the Company

1. Perform duties with responsibility, honesty, integrity, commitment, dedicating physical and mental effort to work, as well as complying with the Company's rules and policies, organizational values, and good traditions, prioritizing the Company's interests.
2. Perform duties in accordance with occupational health, safety, and work environment policies.
3. Strictly maintain the confidentiality of customers, business partners, and the Company by carefully ensuring that documents or confidential information of the Company do not leak or fall into the hands of unrelated parties, which may cause damage to the Company.
4. Do not slander or take any actions that lead to division or internal damage to the Company or persons associated with the Company.
5. Maintain one's honor to be accepted in society, both government agencies and other organizations, and not take any actions that cause damage to the Company's image and reputation.
6. Build good relationships by cooperating with society, communities, government agencies, and related organizations in providing information. Employees at all levels should perform their duties carefully and prudently for the benefit of the Company, the country, and the public.

7. Pay attention to and assist in any actions that will maintain the work environment and atmosphere, including developing the organization toward excellence.
8. Avoid giving and/or receiving gifts, giving and/or receiving entertainment, or any benefits from business partners or persons involved in the Company's business, except for the benefit of conducting the Company's legitimate business or during festivals or customary occasions at appropriate values, whereby recipients should consider according to ethics regarding giving or receiving gifts, property, or any other benefits.
9. Not participate in or conceal any actions that may conflict with the Company's interests or participate in concealing any illegal actions.

Guidelines for Employee Ethics and Code of Conduct comprise:

1. Reporting Non-Compliance with the Code of Conduct
2. Actions Constituting Violations of the Code of Conduct
3. Employee Code of Conduct
4. Procedures for Handling Complaint Reports
5. Protection and Remediation for Reporters or Those Who Cooperate in Reporting

### 1. Reporting Non-Compliance with the Code of Conduct

If any executive or employee observes any matter that constitutes actions not specified in this Employee Code of Conduct, but such actions or omissions may affect the organization's reputation, transparency, and good corporate governance principles, or may conflict with any other Company policies, it shall be the duty of such executive or employee to report such matter to the responsible person. The Company has assigned persons to receive reports of matters not in compliance with the code of conduct and has established reporting channels when non-compliance, violations, or behavior suggesting fraud is observed, as follows:

### Channels for Complaints and Suggestions

Violations or non-compliance with laws, rules, regulations, or conflicts with business ethics or corporate governance principles may be reported through the following channels:

| Type of Report | Report To |
|---|---|
| Employee Code of Conduct Violations | Contact : Human Resources Department<br>Email : Princ_HRwhistle@princgroup.com<br>Website : Contact us at www.principaicapital.co.th<br>Telephone : 02-714-2172<br>Mail : Human Resources Department<br>Principal Capital Public Company Limited<br>29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63, Khlong Tan Nuea, Watthana, Bangkok 10110 |
| Company Director Code of Conduct Violations<br>Financial Reporting Irregularities<br>Matters Affecting the Company's Reputation and Image | Contact : Company Secretary<br>Email : Princ_secretarywhistle@princgroup.com<br>Website : Contact us at www.principaicapital.co.th<br>Telephone : 02-009-2015<br>Mail : Company Secretary<br>Principal Capital Public Company Limited<br>29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63, Khlong Tan Nuea, Watthana, Bangkok 10110 |
| Internal Whistleblowing | Contact : Internal Whistleblowing Committee<br>Email : Princ_internalwhistle@princgroup.com<br>Website : Contact us at www.principaicapital.co.th<br>Mail : Company Secretary<br>Principal Capital Public Company Limited<br>29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63, Khlong Tan Nuea, Watthana, Bangkok 10110 |

### 2. Actions Constituting Violations of the Code of Conduct

All Company executives, employees, and staff have a duty to comply with and promote others' compliance with the code of conduct. However, to prevent violations of the code of conduct that may bring disgrace to the organization, actions constituting violations of the code of conduct are specified for understanding and avoidance as follows:

2.1 Non-compliance with the Company's code of conduct

2.2 Being involved in providing advice, showing channels, encouraging, or supporting others to not comply with the code of conduct

2.3 Neglecting to act or ignoring matters that constitute violations or non-compliance with the code of conduct when one is aware, witnesses, or when it relates to work within one's responsibility

2.4 Not cooperating or obstructing the collection of information for fact-finding investigations regarding complaints of violations or non-compliance with the code of conduct

2.5 Actions that are unfair to other employees arising from reporting or complaining with false statements or one-sided accusations with intent to distort facts for persecution or to create division among the Company's employees

2.6 Observing any other matters that, although not specified in this Employee Code of Conduct, such actions or omissions may affect the organization's reputation, transparency, and good corporate governance principles, or may conflict with any other Company policies, whereby it is equally the employee's duty to report

2.7 Those who violate or do not comply with the code of conduct shall be subject to disciplinary consideration according to the Company's rules and regulations, and in cases where the violation concerns legal provisions, they shall be subject to legal penalties as prescribed by law

## 3. Employee Code of Conduct

### 3.1 Respect for Laws

The Company and all employees must respect laws and stand firm in doing what is right, lawful, and fair, including in conducting business abroad, taking into account the environment, customs, traditions, and culture of each country, comprising:

Guidelines:

1. Company employees must understand laws related to their duties and responsibilities and comply strictly. If uncertain, seek advice from the Company's legal department.
2. Company employees who must work abroad should study the laws, customs, traditions, and culture of the destination country to ensure they do not engage in any illegal actions or actions contrary to the customs and traditions of that country.

### 3.2 Political Activities

The Company is an organization that maintains political neutrality by not engaging in actions that favor any political party, political group, or politician, whether at the national or regional level. The Company supports personnel in adhering to democracy with the King as Head of State, recognizes and respects employees' freedom to exercise their political rights in accordance with the law.

Guidelines:

1. Not use Company resources to support political activities of any political party, political group, or politician, whether directly or indirectly.
2. Avoid serving as a political party director, representing a political party in various public activities, or being a member of local government organizations.
3. Not display any manner that leads others to believe that the Company is involved in or supports political parties.
4. Prohibited from using the Company's authority, resources, and name for solicitation or political activities.
5. Avoid expressing political opinions in the workplace or during work hours that may lead to ideological conflicts.

### 3.3 Protection of Company Assets

Company assets include movable property such as tools, machinery, office equipment, etc., and immovable property such as buildings and land. Additionally, this includes technology, academic knowledge, information, documents, rights, copyrights, patents, as well as the Company's inventions and secrets.

Guidelines:

1. Employees have the duty and responsibility to use Company assets to benefit the Company fully and ensure they are not damaged or lost, and not use Company assets for personal benefit or others' benefit without benefiting the Company.
2. Any research assigned by the Company to personnel to conduct or prepare, or work using information and knowledge learned from the Company, the rights to research, patent applications, patent ownership, and compensation from such work are considered Company property.
3. The Company owns the copyright to computer programs that personnel have been assigned by the Company to develop, including benefits from such programs.

### 3.4 Confidentiality and Use of Inside Information

Confidential information is information that, if disclosed to others at any time, will cause impact to the Company, including the Company's image and reputation. Therefore, employees and Company directors have a duty to keep such information confidential, making it known only to relevant and necessary persons.

Guidelines:

1. Not disclose employees' personal information to other employees or unrelated external parties, unless required by law.
2. Not disclose confidential matters that cannot yet be disclosed at that time, such as operating results and management information not yet publicly disclosed.
3. Not use inside information to benefit oneself or others, such as purchasing Company shares at the time of announcing operating results, purchasing land or investing in businesses near areas where the Company will expand operations.
4. Information disclosure must be by employees assigned by the Company or authorized to disclose such information to ensure disclosed information is accurate and consistent.
5. Not use the Company's computer system to disseminate inappropriate information morally, customarily, or illegally, including forwarding emails that disturb, annoy, or constitute personal business unrelated to the Company's operations.

### 3.5 Conflicts of Interest

Company employees must dedicate themselves to performing their duties considering the Company's interests as primary, not engaging in any actions that create personal benefits or conflicts of interest, and not operating businesses competing with the Company.

Guidelines:

1. Must dedicate oneself to performing duties to the fullest ability. If employees need to work elsewhere for any purpose, that work must be work that:
2. Is lawful or not contrary to laws and good morals
3. Does not conflict with the Company's interests
4. Does not damage the Company's reputation and image
5. Does not use the Company's confidential information
6. Does not affect one's own work duties
7. Facilitates, promotes, and publicizes the Company's image
8. Promotes the application of knowledge gained from such work to develop work for the Company's benefit
9. Not request or receive gifts, property, money, or any other benefits from persons involved in the

Company's business operations

10. Not offer gifts, property, money, or anything else in exchange for personal privileges that should not be received
11. Not issue orders to benefit oneself, both directly and indirectly
12. In meeting deliberations on any agenda, those with interests in that agenda should leave the meeting when considering that agenda
13. Accepting work from affiliated companies is permissible but must be approved by supervisors or management and not demand or receive personal compensation
14. Business entertainment must be practiced reasonably
15. Not operate or invest in any business competing with or similar to the Company's operations, directly or indirectly
16. Recruiting new employees related to current employees must be fair to those with the same qualifications, and employees must not use influence to help hire such employees
17. Avoid purchasing shares or partnering in businesses competing with the Company, which would cause employees to act or omit duties owed to the Company due to concern for their own interests in such businesses
18. Employees must not demand benefits from procurement, purchasing, or hiring, must remain neutral and not engage in any actions that give vendors influence over decisions
19. Prohibited from falsely using the Company's name in transactions unrelated to the Company and avoid conducting transactions using improper methods that damage the Company's reputation or are illegal

### 3.6 Giving and Receiving Gifts

Giving or receiving gifts according to custom is a matter where employees express gratitude or good wishes on various occasions. However, giving and receiving gifts may affect decision-making in performing duties, which may cause the Company to lose benefits.

Guidelines:

1. Receiving gifts should be general in nature, not specific, of reasonable value not exceeding three thousand baht, appropriate to the occasion and season. In cases where employees receive more than one item, employees may choose to receive one item, with the remainder sent to the Human Resources Management Department for lottery among other employees who did not receive gifts.
2. Prohibited from demanding or receiving gifts, property, or any benefits from contractors, subcontractors, customers (both internal customers, meaning employees and other personnel in the Company, and external customers such as insurance companies, construction contractors, etc.), including business partners or persons involved in the Company's operations under any circumstances that may affect

decision-making in performing duties.

3. If employees receive gifts from persons doing business with the Company valued at more than 3,000 baht (three thousand baht), whether designated as personal, but necessary to receive to maintain goodwill, friendship, or good interpersonal relationships, recipients must report to supervisors promptly, and if supervisors determine there is no reason to allow recipients to retain it for personal benefit, recipients must deliver it to supervisors so that property or benefits become the Company's property immediately.
4. Not receive or give gifts in cash, checks, bonds, stocks, gold, gems, real estate, or similar items for personal benefit.
5. Giving gifts and souvenirs should not exceed three thousand baht in value.

### 3.7 Conduct Toward the Company and Conduct Toward Employees

Employees are valuable assets of the Company. Living together in an organization with diverse cultures and professions, ethnicities, and religions requires promoting employee harmony, treating each other politely and respectfully within the framework of established policies and practices. The established code of conduct may not cover every case that may arise. Therefore, when employees face new problems or increasingly complex cases, employees should consult with direct supervisors or supervisors in their own line of work. The Company considers direct supervisors as Company representatives in providing advice and guidance for solving various problems, with the Company's Human Resources service unit as the ultimate resource.

Guidelines:

1. Treat everyone equally, without discrimination, without segregating race, religion, status, education, or any other status not directly related to performing duties.
2. Employees must follow the chain of command, receive orders, and be directly responsible for work to direct supervisors in the line of work, not bypassing the chain of command unless necessary.
3. Avoid criticizing supervisors and colleagues in ways that cause damage to such persons and create division among employee groups.
4. Must have polite manners, dress appropriately for the occasion, conduct oneself appropriately for work duties, maintain one's honor to be accepted in society, and maintain the Company's image.
5. Conduct oneself according to rules, regulations, and good customs correctly and appropriately, whether specified in writing or not, must have discipline and consciousness to conduct oneself in this manner at all times.
6. When facing new problems or cases that are too complex for employees' capabilities, employees should consult direct supervisors or supervisors in their own line of work in hierarchical order.

## 4. Procedures for Handling Complaint Reports

Those assigned to receive the above complaints must undertake the following:

4.1 Collect actual relevant information regarding violations, omissions, or non-compliance with the code of conduct, whereby those overseeing relevant information must disclose all information to those collecting information and investigating complaints.

4.2 Process and analyze data results to determine the root cause of whether there were any actions that violated, omitted, or failed to comply with the code of conduct, and report the data processing and analysis to those authorized to issue orders on such matters.

4.3 Report facts to the Board of Directors to investigate facts and establish action measures to stop violations or non-compliance with the Company's code of conduct.

4.4 Notify complainants of results if complainants disclose their identity.

4.5 In cases of important matters that may have a material impact and cause significant damage to the Company, those responsible should report to the Chief Executive Officer and Chairman of the Executive Committee for consideration of reporting to the Board of Directors for acknowledgment.

## 5. Protection and Remediation for Reporters or Those Who Cooperate in Reporting

Reporters or those who cooperate in fact-finding investigations must receive protection and fairness, whereby the Company has established the following criteria:

5.1 Complainants may choose not to disclose their identity if they believe disclosure would be unsafe; however, if they disclose their identity, they will receive progress reports and factual clarifications, or remediation of actual damages more conveniently and expeditiously.

5.2 Those assigned to receive complaints shall maintain confidentiality of relevant information and disclose only as necessary, taking into consideration the safety and potential harm to reporters or those cooperating in information verification, whereby the Company guarantees that such reporting will not constitute grounds or be considered grounds for termination, disciplinary action, or any adverse action against such employees.

5.3 Those who have suffered harm will receive remediation through appropriate and fair processes.

## 6. Disciplinary Action

The Company will consider disciplinary action according to the Company's regulations. In cases of law violations, the Company will proceed to refer the matter to government officials for further legal action.

## 1) Investor Relations Code of Conduct

The Investor Relations Code of Conduct is prepared to serve as a guideline or framework for establishing the Company's investor relations code of conduct, comprising two parts:

1) Fundamental Principles: Key principles that investor relations professionals should adhere to as a framework for performing duties. When facing difficult issues or decisions, investor relations professionals should seek alternatives that do not conflict with these fundamental principles.
2) Practices According to Fundamental Principles: Guidelines to help investor relations professionals perform duties consistent with fundamental principles. Investor relations professionals should consider appropriateness and may establish additional practices to ensure investor relations work is conducted equitably and fairly.

**Fundamental Principles**

1. Investor relations professionals must disclose material and necessary information for investment decisions accurately, adequately, and in a timely manner.
2. Investor relations professionals must not use inside information for personal benefit or the benefit of others.
3. Investor relations professionals must disclose information equitably and fairly by providing opportunities for all relevant groups to access and inquire about information.
4. Investor relations professionals must perform duties with professional integrity based on the principle of equality, without discrimination based on any monetary inducements that constitute personal motivation and self-interest over the Company's interests and related stakeholders.

**Practices According to Fundamental Principles**

1. Disclosure of Material and Necessary Information Accurately, Adequately, and in a Timely Manner

    1.1 Investor relations professionals must disclose information accurately, adequately, and in a timely manner by complying with requirements of regulatory agencies such as the SEC and the Stock Exchange of Thailand.

    1.2 Investor relations professionals should exercise judgment in providing information carefully and prudently, whereby investor relations professionals may refuse to provide information if, upon consideration, such information is deemed trade secrets or information that may cause the Company to lose competitive advantage.

    1.3 Investor relations professionals should consider providing information with clarity and sufficient detail for understanding, such as clarifying information or reasons causing the Company's operating results to change by more than 20%, and/or information in MD&A should have clear explanations that enable understanding of the background and reasons for changes in various figures.

    1.4 In cases of rumors or leaked information, investor relations professionals should promptly clarify facts to

the public by complying with the Stock Exchange of Thailand's requirements regarding listed company information disclosure.

1.5 Investor relations professionals should not intentionally disclose inaccurate information to promote purchasing of Company shares.

1.6 Investor relations professionals should establish channels for information disclosure or information sources for users to receive information equally.

2. Protection and Maintenance of Inside Information

2.1 Listed companies should establish guidelines for protecting inside information, such as defining and limiting persons who can access inside information, whereby investor relations professionals with access to inside information must not disclose such information to others until such information is publicly disclosed according to various regulations.

2.2 Investor relations professionals must comply with regulations related to protecting inside information correctly, such as material information affecting operating results should be disclosed through the Stock Exchange of Thailand's channels for general knowledge before disclosure to any specific investor group.

2.3 Listed companies should establish criteria for trading Company shares for investor relations professionals, such as establishing blackout periods for trading shares and reporting share trading to the Compliance department or other assigned departments such as the Company Secretary.

2.4 Investor relations professionals should establish a quiet period for refraining from scheduling meetings or answering questions about future operating results for analysts and investors. Since investor relations professionals at each company begin receiving financial statement information at different times, investor relations professionals should consider establishing quiet periods appropriately and as close as possible to the time of receiving figures, such as at least two weeks before financial statement disclosure.

2.5 In cases of organizing analyst meetings before financial statement announcements (Earnings Preview), investor relations professionals should complete such meetings before the quiet period and should be cautious in providing information by not providing any prohibited information, such as estimated revenue and profit figures for that financial period.

3. Equitable and Fair Information Disclosure

3.1 Investor relations professionals must provide opportunities for stakeholders to access information equally. The format of activities organized for each group may differ as appropriate, but the information provided must be equal and not disadvantage any party or cause loss of investment opportunities.

3.2 Investor relations professionals should provide opportunities for stakeholders to contact and inquire as appropriate, without discriminating by contacting only certain specific groups.

3.3 Investor relations professionals should disclose information presented in exclusive meetings to the public

generally and as soon as possible, such as posting Roadshow Presentations and Analyst Presentations on the Company's website promptly after meetings conclude.

3.4 Investor relations professionals should exercise caution in communicating information through social networks. Investor relations professionals can follow information to help understand investor perspectives, but if issues arise causing misunderstanding requiring clarification, investor relations professionals should provide information through the Stock Exchange of Thailand's system for all parties to receive generally, to prevent problems of providing information to specific groups.

3.5 Investor relations professionals should treat each stakeholder group as follows:

3.5.1 Treatment of Investors

- Investor relations professionals should treat all investors equally, whether large or small investors.
- Investor relations professionals should provide opportunities for individual investors to access information at levels equal to analysts and institutional investors.
- Investor relations professionals should not discontinue the practice of accepting one-on-one meetings with institutional investors or investor groups. If unable to meet with all groups, investor relations professionals should establish clear and fair criteria for accepting meetings.
- In organizing activities for investors, such as site visits and investor meetings, investor relations professionals should proceed by considering the Company's benefits and cost-effectiveness of resources to be used as primary considerations.

3.5.2 Treatment of Analysts

- In analyst meetings, investor relations professionals should invite and provide opportunities for analysts from all securities companies to participate equally.
- Investor relations professionals should not provide compensation or gifts to analysts to induce or persuade them to write research reports for the Company and/or to write only positive research reports.
- Investor relations professionals should respect analysts' work and opinions but may clarify correct facts if inaccurate information is used or provided.

3.5.3 Treatment of Media

- Investor relations professionals should provide information and opportunities for media to receive information appropriately.

- Investor relations professionals should not use business conditions with media, such as advertising in media, to have media present news or provide positive opinions about the Company.
- Investor relations professionals should not provide compensation or gifts to media to induce or persuade media to write articles or news for the Company creating false news.

3.5.4 Treatment of Regulatory Agencies

- Investor relations professionals should cooperate in providing information to regulatory agencies as requested.

3.5.5 Treatment of Internal Organizational Personnel

- Investor relations professionals should coordinate for Company management to meet with various stakeholders at appropriate opportunities.
- Investor relations professionals should report to the Board of Directors and management regarding information that will help create added value for the Company, such as investor relations activity performance results, opinions from analysts and investors, and capital market movement information.

3.5.6 Treatment of Other Stakeholders such as Financial Institutions and Credit Rating Companies

- Investor relations professionals should provide information to other stakeholders at equal levels, except when necessary for business operations, such as providing inside information for project credit applications from financial institutions. In such cases, investor relations professionals must proceed cautiously and must require those receiving inside information to sign confidentiality agreements.

4. Performing Duties with Integrity

4.1 Investor relations professionals should avoid any actions contrary to the Company's interests, such as using Company assets or information for personal benefit.

4.2 Investor relations professionals should not seek personal benefits from relationships and information obtained from performing investor relations duties for the Company.

4.3 Investor relations professionals must not prioritize personal interests in any form in selecting or participating in activities with external organizations, such as selecting to participate in roadshows only with certain securities companies providing special privileges.

4.4 Investor relations professionals should comply with various employee policies and codes of conduct established by the Company.

5. Other Matters

5.1 Investor relations professionals should dress appropriately for venues and activities attended.

5.2 Investor relations professionals should not provide negative information or defame competitor companies or various stakeholders.

## 2) BUSINESS ETHICS

### 2.1 Ethics Toward Stakeholders

With a commitment to promoting the Company as an efficient organization that is responsible to its stakeholders in both business operations and personnel matters, the Company has established guidelines for the Board of Directors, specialized committees, executives, and employees to uphold as the foundation for their work, as follows:

**1. Ethics Toward Shareholders**

1.1 Perform duties with honesty and integrity, and make decisions with good faith and fairness toward all shareholders, both large and small, and for the benefit of all related stakeholder groups.

1.2 Manage the Company's affairs to ensure progress, stability, and generate appropriate returns for shareholders.

1.3 Perform duties and make decisions with capability and prudence by applying knowledge, experience, expertise, and management skills to the best of one's ability in all circumstances.

1.4 Report the Company's status and operational results to shareholders equally, regularly, and completely in accordance with the facts.

1.5 Not seek benefits for oneself or related parties by using any information of the Company that has not yet been disclosed to the public.

1.6 Not disclose confidential information of the Company to others improperly.

1.7 Not undertake any actions that may cause conflicts of interest with the Company.

**2. Ethics Toward Customers**

2.1 Develop real estate business related to the Company's operations and provide quality services in compliance with contracts, agreements, or various terms with customers in a transparent and equal manner. In cases where performance cannot be fulfilled, promptly negotiate with customers in advance to jointly find solutions and prevent damage.

2.2 Commit to creating satisfaction and confidence for customers to receive excellent quality service

under safe conditions and appropriate technology, as well as continuously elevate standards to higher levels.

2.3 Disclose information about services completely, accurately, in a timely manner, and without distorting facts, as well as maintain good and sustainable relationships.

2.4 Establish customer service systems and open communication channels so that customers can file complaints about dissatisfaction and take the best actions to respond to customer needs quickly.

2.5 Emphasize the importance of maintaining customer confidential information regularly and not use such information for the benefit of oneself and/or other related parties.

3. Ethics Toward Competitors

3.1 Treat competitors equally and fairly, based on the foundation of receiving fair returns for both parties.

3.2 Conduct business within the framework of fair competition rules.

3.3 Not seek competitors' confidential information through dishonest or inappropriate methods.

3.4 Not damage competitors' reputation by making false accusations without truth.

4. Ethics Toward Creditors

4.1 Strictly, transparently, and equally comply with contracts, agreements, and various terms with creditors.

4.2 Report the Company's financial position honestly, accurately, and timely to creditors regularly.

4.3 In cases where conditions cannot be met, promptly notify and negotiate with creditors in advance to jointly find solutions and prevent damage.

5. Ethics Toward Employees

5.1 Provide fair and appropriate compensation according to the knowledge, ability, responsibility, and work performance of each employee.

5.2 Appointments, transfers, rewards, and disciplinary actions toward employees must be conducted with equality, good faith, and based on the foundation of knowledge, ability, and appropriateness, as well as the actions or performance of such employees.

5.3 Treat employees on the basis of justice and emphasize the development and transfer of knowledge and abilities to employees by providing opportunities to employees thoroughly and regularly.

5.4 Strictly comply with laws and regulations related to employees.

5.5 Maintain work environment conditions to ensure safety for the life, health, body, and property of employees at all times.

5.6 Manage operations by avoiding any unfair actions that may affect the stability of employees' performance of duties.

5.7 Listen to opinions and suggestions from employees at all levels equally and fairly.

5.8 Promote employee understanding of ethics and roles to encourage ethical behavior throughout the

Company.

5.9 Encourage employees to participate in determining work direction, including solving problems of departments and the Company as a whole.

5.10 Promote employees to receive additional training in fields related to their job duties.

5.11 Promote employees to be good people with virtue and comply with the law.

**6. Ethics Toward Community, Society, and Environment**

6.1 Not undertake any actions that cause damage to natural resources and the environment beyond what is required by law.

6.2 Not support any activities that are harmful to society or good morals and/or promote vices.

6.3 Emphasize community and social activities, focusing on the development of society, community, and environment with a focus on creation and conservation of natural resources.

6.4 Support activities that create public benefits, such as reducing energy and natural resource consumption.

6.5 Instill awareness of responsibility toward society and the environment in the Company and employees at all levels continuously.

6.6 Cooperate and strictly control compliance with the spirit of laws and related regulations.

6.7 Respond quickly and effectively to events that impact the community and environment resulting from the Company's operations by fully cooperating with government officials and related agencies.

6.8 Establish a grievance system for matters that may affect the community, investigate causes, improve and correct, and inform complainants of operational results in a timely manner.

6.9 Promote efficient energy conservation for the benefit of future generations.

**7. Supplier Code of Conduct**

7.1 Business Ethics with Honesty and Transparency (Business Integrity)

7.1.1 Corporate Governance

The Company's suppliers must comply with laws, rules, and regulations related to business operations with honesty, integrity, transparency, and accountability, considering stakeholders under good corporate governance principles.

7.1.2 Confidentiality and Personal Data Protection

The Company's suppliers must keep information of the Company and related parties in the business confidential and not use, collect, or disclose such information without consent, including taking action to ensure data owners receive comprehensive protection of their rights in accordance with the law.

7.1.3 Respect for Intellectual Property

The Company's suppliers must respect and not infringe upon the intellectual property of

others, including establishing measures to prevent intellectual property infringement.

7.1.4 Avoidance of Conflicts of Interest

The Company adheres to virtue and ethics in business operations and is well aware that organizations lacking virtue and ethics cannot maintain sustainability in business. The Company therefore expects suppliers to practice in the same manner by not undertaking any actions that create conflicts of interest or have vested interests between suppliers and the Company's personnel.

7.1.5 Giving of Gifts, Gratuities, or Entertainment

The Company's suppliers must not offer gifts, gratuities, bribes, fees, services, discounts, other special privileges, including any benefits or entertainment to employees or executives of the Company that may be interpreted as improperly and unfairly benefiting the supplier.

7.1.6 Use of Insider Information (Insider Trading)

The Company's suppliers must not use information not disclosed to the public that they receive during transactions with the Company for personal benefit of the supplier itself, supplier's employees, or any other person.

7.1.7 Anti-Corruption

The Company's suppliers shall not commit or support fraud or corruption in any form by establishing anti-corruption measures, internal controls, and internal audits, including cooperating with the Company to prevent and suppress fraud or corruption, as well as participating in the declaration of intent and requesting certification of membership in the Thai Private Sector Collective Action Against Corruption (CAC).

7.1.8 Fair Practices

The Company's suppliers shall be responsible for treating all stakeholders fairly, including complying with trade competition laws to ensure fair competition, not causing disadvantage to others for oneself or any person to receive benefits that should not be obtained.

7.2 Labor Practices and Human Rights

7.2.1 Non-Discrimination

The Company's suppliers must consider human dignity, equality, and fairness by not discriminating against workers due to physical or mental differences, race, nationality, religion, gender, age, education, disability, or any other matter.

7.2.2 Compliance with Labor Laws

The Company's suppliers must treat workers in accordance with labor laws and human

rights principles correctly and completely, provide freedom of association and the right to collective bargaining according to law, including having termination processes in accordance with labor law.

7.2.3 Protection of Child Labor

The Company's suppliers must demonstrate responsibility as employers who treat employees and provide employees with protection as legally required, with workers being no less than 15 years old. In cases of employing child labor aged 15 years or older but not exceeding 18 years, such workers must be provided with protection, wages, benefits, or any other matters according to legal rights in all respects.

7.2.4 Protection of Female Workers

Suppliers must ensure that female employees and pregnant women do not work in areas dangerous to health and safety. Pregnant women must receive protection and benefits as prescribed by law. Suppliers must not terminate employment, reduce job positions, or reduce employee benefits due to pregnancy.

7.2.5 Forced Labor

Suppliers must not commit physical coercion, punishment, intimidation, detention, threats, abuse, human trafficking, use of violence in any form, or use contracts to bind workers. Suppliers must ensure that employment is voluntary. Suppliers must not request that employees perform work involuntarily and allow them to resign when they wish. Suppliers must not collect money or government documents, legal documents of employees (such as national identity cards, passports, or work permits) as work security, unless it is an action that does not violate the law.

7.2.6 Management of Wages, Benefits, and Working Hours

The Company's suppliers must manage wages, compensation, overtime pay, benefits, working hours, and welfare correctly according to law, on time, and equally for equal work without any discrimination. They must not allow employees to work longer than legally required. If necessary, it must be voluntary on the part of employees.

7.3 Occupational Health and Safety

7.3.1 Safety and Work Environment

The Company's suppliers must strictly comply with safety and occupational health laws, prepare work environments to be safe and hygienic to reduce and control potential injuries/illnesses/accidents and emergencies, provide training and create awareness to reduce and control accident risks, as well as provide opportunities for their employees to present safety issues without being considered as actions contrary to disciplinary

regulations.

7.3.2 Personal Protective Equipment

The Company's suppliers must prepare personal protective equipment that is ready to use, appropriate for work, and sufficient for their employees.

7.3.3 Emergency Preparedness

The Company's suppliers must assess situations and emergencies, have plans and procedures to support and respond to emergency situations, and provide continuous training and communication to their employees to ensure employees understand and can perform correctly and safely when emergency situations occur.

7.4 Social Development Participation

7.4.1 The Company's suppliers should operate business considering potential impacts on surrounding communities and society, and participate in developing quality of life, creating better living conditions for communities and Thai society.

7.4.2 The Company's suppliers should choose products and services that promote the community's economy or jointly develop products from communities to create careers and extend wisdom from community ways of life.

7.5 Environment

7.5.1 The Company's suppliers must comply with environmental laws, regulations, and rules, including managing pollution/waste as required by law.

7.5.2 The Company's suppliers should use resources economically, use the 3 Rs principles: Reduce, Reuse, and Recycle.

7.5.3 The Company's suppliers should choose environmentally friendly products and services and be cautious in any actions that impact the environment.

7.5.4 The Company's suppliers should have policies and/or operational guidelines that monitor and disclose greenhouse gas emissions according to accepted standards.

7.5.5 The Company's suppliers should promote policies, targets, or plans to reduce environmental impacts and reduce greenhouse gas emissions.

7.5.6 The Company's suppliers should enhance knowledge and awareness of management to reduce impacts on the environment and climate to their own employees, suppliers, and stakeholders.

7.6 Subcontractors and Business Partners of Suppliers

7.6.1 The Company's suppliers must make their best efforts to inspect the operations of subcontractors and business partners of suppliers to ensure such persons have work that complies with this code of conduct. Suppliers should assess risks that may arise if

operations may deviate from this code of conduct and must have plans to improve, correct, or terminate business participation with subcontractors and business partners of suppliers.

7.7 Inspection/Data Collection

7.7.1 The Company's suppliers must make their best efforts to provide audit documentation and appropriately store such information to demonstrate compliance with this code of conduct.

7.7.2 The Company's suppliers must provide audit documentation for operating procedures that comply with this code of conduct, both for themselves and business partners of suppliers, and can submit such documents to the Company in case of request.

7.7.3 Suppliers must make their best efforts to inspect the operations of subcontractors and business partners of suppliers to ensure such persons have work that complies with this code of conduct. Suppliers should assess risks that may arise if operations may deviate from this code of conduct and must have plans to improve, correct, or terminate business participation with subcontractors and business partners of suppliers.

## 2.2 Ethics Regarding Respect for Law and Universal Human Rights Principles

1. Employees at all levels of the Company must thoroughly understand the laws related to their duties and direct responsibilities and comply with them strictly. If uncertain, seek advice from the Legal Department. Do not act according to one's own understanding without guidance.
2. The Company compiles laws, government rules, and regulations by category for employees to study and provides appropriate legal training to employees related to their duties.
3. The Company must strictly comply with universal human rights principles, provide knowledge and understanding of universal human rights principles to employees for implementation as part of operations, and not support businesses that violate universal human rights principles.
4. When employees must perform work in foreign countries, employees should study the laws, customs, traditions, and culture of the destination country before travel to ensure that the Company's various projects, services, equipment, and accompanying documents, including travel documents, purpose of travel, and work performance in the destination country do not violate laws or contradict the customs, traditions, and culture of the destination country.

## 2.3 Ethics Regarding Culture, Customs, Traditions, and Political Neutrality

The Company respects differences in culture and local customs and traditions by not undertaking any actions that are contrary to such culture and customs and traditions, with the following guidelines:

1. The Company emphasizes political neutrality and does not participate in or show favoritism toward

any particular political party or any individual with political power.

2. The Company does not use the Company's capital or resources to support any political party or politicians, either directly or indirectly.
3. The Company does not participate in campaigning or advertising for any political party or politicians on Company premises, including not using the Company's resources and property for such purposes.
4. The Company encourages employees at all levels to exercise their voting rights according to the constitution. The Company has no policy to provide financial support, either directly or indirectly, to any politicians or political parties for the benefit of such politicians or political parties.
5. Employees at all levels of the Company may exercise their political rights as individuals, and shall not use their position in the Company or the Company's name or logo to persuade others to donate money or provide support to any politicians or political parties.
6. Adhere to democratic principles and encourage employees to exercise their voting rights according to the constitution.

### 2.4 Ethics Regarding Conflicts of Interest

Any actions of the Company shall uphold the Company's interests as paramount and shall not be involved in activities that may cause conflicts of interest, with the following guidelines:

1. Employees at all levels of the Company must make decisions regarding the Company's business operations for the maximum benefit of the Company.
2. Any actions and decisions of employees at all levels must be free from the influence of personal desires or those of persons related to such employees, whether by blood or other persons specifically known personally, and use fair and appropriate prices as if conducting transactions with external parties. When making decisions or approving transactions that may have conflicts of interest, report to supervisors or those involved in approval and withdraw from participation in such transactions.
3. Employees at all levels of the Company must comply with the Company's procedures according to the same standards by working full-time for the Company to the best of their ability without diverting time from work to conduct other external businesses unrelated to the Company's interests.
4. Employees at all levels of the Company must avoid financial involvement and/or relationships with other external parties that would cause the Company to lose benefits or cause conflicts of interest or obstruct efficient work performance.
5. The performance of duties and holding of positions by the Company's directors, specialized committees, executives, and all employees must not conflict with the Company's main interests.

### 2.5 Ethics Regarding Related Party Transactions

The Company adheres to the following guidelines in conducting operations to ensure related party transactions are in accordance with normal business practices and are of maximum benefit to the Company:

1. The Board of Directors must perform duties in compliance with the Securities and Exchange Act and the regulations, notifications, orders, or requirements of the Stock Exchange of Thailand, including compliance with requirements regarding disclosure of related party transactions and acquisition or disposal of significant assets of the Company according to accounting standards prescribed by the Federation of Accounting Professions.
2. Related party transactions under the notifications of the Stock Exchange of Thailand must strictly comply with the criteria, methods, and disclosure of related information.
3. In cases where it is necessary to conduct transactions related to oneself, consider the Company's interests as primary and conduct such transactions as if conducting transactions with external parties. Directors, executives, and all employees involved in such transactions must not participate in consideration for approval and must report their vested interests to the Board of Directors and/or supervisors for acknowledgment.

### 2.6 Ethics Regarding Confidentiality and Use of Insider Information

Protection of insider information is extremely important to the Company's success, as well as to the career security of all employees. To ensure that providing information to external parties is conducted in a manner that will not cause damage to the business and reputation of the Company, the following ethics regarding confidentiality and use of insider information are established:

1. Employees at all levels of the Company should maintain insider information and documents that cannot be disclosed to external parties, which leads to seeking benefits for oneself, family, or associates improperly, such as information that affects stock prices, trade secrets, various invention formulas, which are considered the Company's rights.
2. Employees at all levels of the Company shall not use confidential information for personal benefit or that of other persons.
3. Employees at all levels of the Company who receive personal data must carefully store or use such information.
4. The Company stipulates that information related to contractual parties and agreements with contractual parties are considered confidential and cannot be disclosed to other persons unless authorized by the Company and the contractual party only.
5. The Company should establish measures and control systems for Company information within departments or divisions strictly to prevent important insider information of the Company from being disclosed externally before official publication. Such measures and control systems are considered part of the Company's important risk control measures.
6. The Company assigns as the duty and responsibility of supervisors at various levels to control and ensure that there is no leakage of the Company's important information and news externally by employees under their supervision before

the Company's official disclosure of information.

7. The sharing of insider information among employees must be within the scope of duties and responsibilities only as employees are assigned.
8. Employees at all levels of the Company shall not disclose the Company's confidential information even after termination or cessation of duties.

### 2.7 Ethics Regarding Giving or Receiving Gifts, Property, or Other Benefits

The Company stipulates that giving or receiving gifts, property, or other benefits shall be in accordance with reasonable actions but must not influence the Company's decisions. The following guidelines are established:

1. Employees at all levels and/or family members shall not demand gifts, property, or other benefits from contractors, traders, vendors, joint venture partners, or those involved with the Company's business under any circumstances whatsoever.
2. In cases where supervisors consider it inappropriate to receive gifts, property, or other benefits, return them to the giver immediately. If unable to return, submit to the supervisor to become the Company's property.
3. Gifts given to the Company that have value for commemorating important events of the Company, such as when signing joint venture contracts of the Company, when receiving various awards, or souvenirs from participating in social assistance activities, etc., employees at all levels are allowed to receive on behalf of the Company.
4. Employees at all levels of the Company should not give gifts to supervisors, and supervisors shall not consent to or knowingly allow their relatives to receive gifts from employees under their supervision, except in cases of normal customs where gifts are exchanged, but must have a price or value not exceeding 3,000 baht (three thousand baht).
5. In cases of receiving property or other benefits, whether from domestic or foreign sources with a value not exceeding 3,000 baht (three thousand baht), whether specified as personal or not, but necessary to receive to maintain goodwill, friendship, or good personal relationships, the recipient must report to the supervisor promptly, and if the supervisor deems there is no reason to allow the recipient to retain it for personal benefit, the recipient must submit it to the supervisor for such property or benefit to become the Company's property immediately.
6. Employees at all levels of the Company should not give, receive, or promise to give or receive benefits or anything of value to induce action or omission of action, including any actions that fall under such circumstances.
7. Receiving gifts or giveaways such as calendar sets or notebook sets with a value not exceeding three thousand baht.

8. Giving gifts or giveaways such as calendar sets or notebook sets with a value not exceeding three thousand baht.

### 2.8 Ethics Regarding Marketing Communications

Marketing communications play an important role in creating good values of the Company to society by introducing the Company's innovations to the public. The Company has established guidelines for marketing communications practices as follows:

1. The Company should refrain from providing distorted or incomplete information.
2. The Company should refrain from false advertising or advertising that may cause misunderstanding.
3. The Company should refrain from advertising or providing news to the mass media that distorts the truth or violates culture, good morals, or defames competitors whether directly or indirectly.

### 2.9 Ethics Regarding Intellectual Property

Intellectual property is considered one of the Company's most valuable assets and is important for maintaining competitive advantage in business. Brand identity consists of the Company's name, logo, copyrights, patents, trademarks, service marks, trade secrets, work procedures, innovations, content, and various legitimate rights. It is extremely important that the Company protects these assets and respects such property of others. The following guidelines are established:

1. The Company must conduct business in accordance with laws, regulations, and contractual obligations related to legitimate intellectual property rights, including patents, copyrights, trade secrets, and other proprietary information.
2. The Company shall not infringe upon or misuse legitimate intellectual property rights.
3. Employees at all levels of the Company who are responsible for maintaining trade secrets, secret trade formulas, work processes, or confidential business methods must maintain such secrets as safely as possible and prevent such information from leaking.
4. Employees at all levels of the Company must respect the intellectual property rights of others and not use the work of others, even partially, for personal benefit without permission or without providing compensation to the owner beforehand.

### 2.10 Ethics Regarding Use of Information Technology and Communications

The Company provides information technology and communications for use in conducting business. Employees at all levels must use these things correctly and efficiently for the maximum benefit of the Company and be careful not to cause impact to the Company or stakeholders. The Company has established guidelines for the use of information technology and communications as follows:

1. Employees at all levels of the Company must perform work using properly licensed computer programs. If performing duties on computers outside the office, verify licenses every time. Absolutely prohibit installation or use of improperly licensed computer programs in the office.
2. Employees at all levels of the Company must keep their passwords confidential and not tell other persons to prevent other persons from accessing their passwords, as well as not use the internet or access unfamiliar websites that may cause danger to the Company's computer system.

## 3) INTERNAL CONTROL POLICY

The Company has a policy for all departments to operate systematically, efficiently, and effectively in accordance with the Company's objectives and goals, to maintain and use assets economically and appropriately, and to have a comprehensive, continuous, and effective internal control system including risk assessment and management. Department owners must have good standard operating systems and internal controls to prevent undesirable events that may cause damage to the Company, and develop employees in the department to share a sense of commitment to perform work according to appropriate work procedures, including relevant regulations and laws, and be ready to allow the Company to evaluate and inspect work at all times. The Company has the following operational guidelines:

1. It is established as the duty and responsibility of executives at all levels to oversee and inspect the work systems within their departments to be efficient and correct according to operational regulations, with a comprehensive and auditable internal control system. Every department must prepare a manual defining operational regulations as standards for conducting business in the work areas under their supervision, adhering to the Company's quality policy, important policies, and other practices related to corporate governance principles.
2. Internal control guidelines that include risk assessment and management control are guidelines that will help each department assess risks in the work for which they are responsible and find ways to control by reducing impact or reducing the likelihood of such risks occurring. The Company wants employees at all levels to participate in risk assessment and control generally to help prevent damage that may occur.
3. Internal auditors will support executives of all departments in establishing internal controls in every department and conduct periodic inspections as appropriate to ensure that all departments have effective internal control systems and continuously comply with established procedures, which will lead to improving

work systems to be even more efficient.

4. The audit and evaluation approach will emphasize constructive improvement of work systems. Reports prepared by internal auditors, with which the system-owning parties have agreed, will be submitted to the Audit Committee for approval before further implementation. If it appears that any department's work system needs to be improved or made more efficient or comprehensive, all related departments are obligated to promptly implement improvements. The Company will consider such duties as part of the work for which such departments are responsible and as part of the performance evaluation of the persons involved.

## 4) RISK MANAGEMENT POLICY

### 1. Background and Importance

To ensure the Company's operations are consistent with good governance principles and to provide reasonable assurance that what is being implemented is correct and appropriate, promotes the value and worth of the business, and is in accordance with the COSO internal control framework of the Securities and Exchange Commission, the Company emphasizes the risk management process, from identifying, analyzing, and assessing risks, to managing and controlling risks, as well as monitoring and reporting results. The Company has adopted risk management guidelines according to ISO 9001:2015 standards to develop a risk management framework. "Risk" means the impact from uncertainty and changes that will cause operations to not achieve the business objectives and goals.

### 2. Objectives

(1) To declare the intent and goals of risk management, as well as the operational framework in the risk management process, which will be used within the Company.

(2) To ensure all personnel at all levels in the Company are aware of their roles, responsibilities, and operational guidelines in risk management to ensure operations achieve the Company's goals.

### 3. Risk Management Guidelines

(1) The Company operates its business under six risk areas: investment, finance, operations, politics and government policy, good corporate governance and law, and reputation and image. Therefore, the Company needs to have systematic and continuous risk management at both the organizational and project levels, using the same standards as determined by the Company.

(2) Executives must communicate to personnel in all departments about the importance of risk management and the Company's risks. Company personnel must be able to demonstrate the risk status of related work

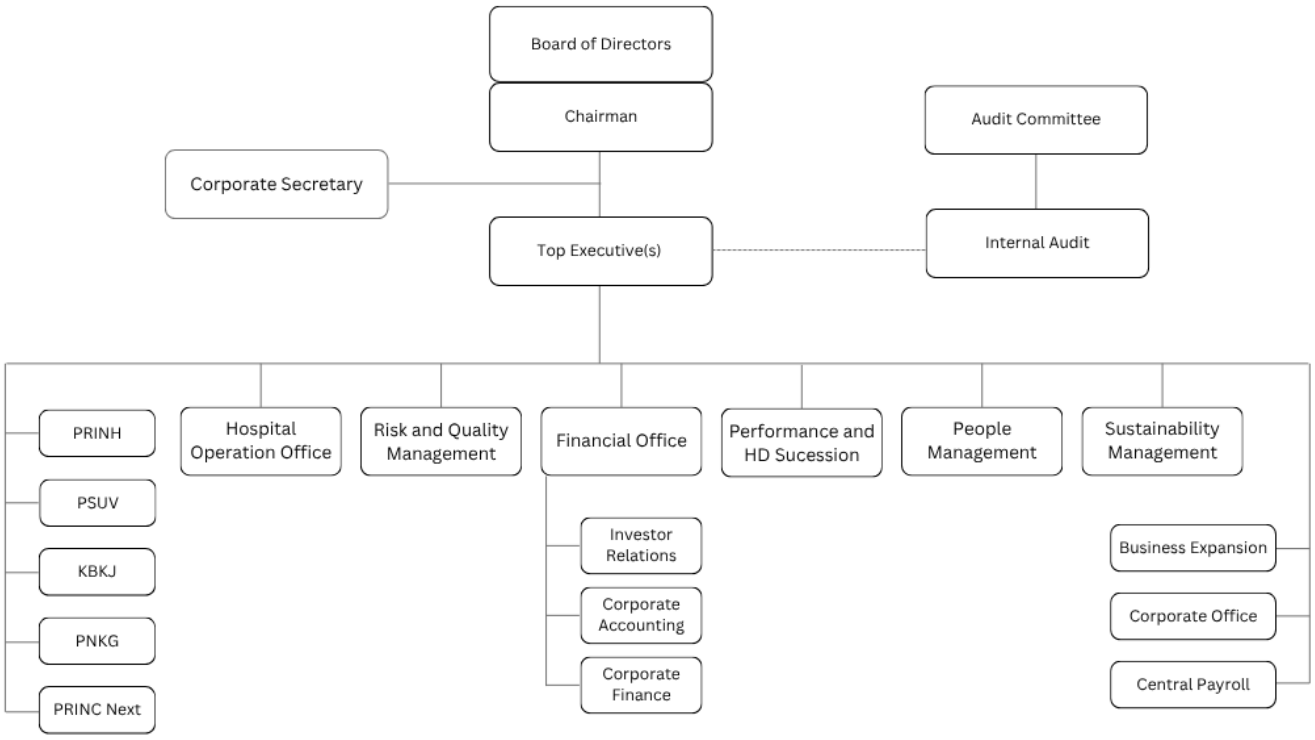
and use it in decision-making to manage departments, including establishing appropriate operational guidelines and emergency contingency plans to deal with such risks.

(3) Each department shall use risk maps and risk management tools according to the Risk Management Manual to identify risk factors and types of risks that affect operations, analyze and assess discovered risks, determine risk levels along with acceptable criteria, establish operational guidelines/measures or risk management plans to prevent, mitigate, avoid, or effectively control risks, as well as supervise, monitor, review, and evaluate risk management results to improve the risk management process to be progressively more effective.

(4) Each department's responsible persons shall report monitoring and evaluation results of risk management as determined by the Company to the Risk Management Committee.

(5) The Risk Management Committee establishes risk management policies and operational guidelines, including supervising and monitoring risks within the organization, and will summarize and report risk management results to the Board of Directors.

## 4. โครงสร้างการบริหารความเสี่ยงและหน้าที่ความรับผิดชอบ




(1) Board of Directors has the responsibility for overall supervision of the Company's risk management.

(2) Audit Committee has the function of supporting the Board of Directors through independent review to ensure the risk management system is appropriate and effective.

(3) Executive Committee has the responsibility to review, supervise, and monitor the business's significant risk status and the Company's internal control system.

(4) Managing Director has the responsibility to implement risk management policies, supervise the risk management process to be continuously practiced throughout the organization, and ensure there are appropriate risk management plans.

(5) Risk Management Committee has responsibilities covering the following matters:

(5.1) Establish risk management policies, goals, and strategies.

(5.2) Develop enterprise-wide risk management systems to be efficient and drive continuous cooperation in risk management at all levels.

(5.3) Monitor and review risks of various departments and provide recommendations and corrective guidelines.

(5.4) Supervise the effectiveness of the risk management process.

(5.5) Report risks and risk management results to the Board of Directors meeting according to the established agenda.

(5.6) Appoint sub-working groups and supervise the appointed working groups to perform duties as assigned.

## 5. Risk Management Methods

The Company has adopted risk management guidelines consistent with ISO 9001:2015 standards as a model for developing an operational framework for risk management throughout the organization.

## 6. Expected Outcomes from Risk Management

(1) Create awareness of the need for proactive risk management by identifying, assessing, and managing risks seriously and comprehensively throughout the organization.

(2) Increase channels for identifying opportunities that may lead to business growth and be prepared for threats that will be obstacles to operations.

(3) Have risk management that meets international standards.

(4) Increase opportunities and possibilities for operational results that achieve goals, which will bring confidence and trust from stakeholders to the business.

(5) Be able to use risk information in strategic planning and decision-making.

(6) Make strategic plan implementation clearer and more predictable.

(7) Increase the ability to manage incidents better.

(8) Increase learning from experience in managing risks.

### 7. Policy Review

The Risk Management Committee must review the risk management policy and related documentation at least once a year, reporting the appropriateness and effectiveness of implementation to the Board of Directors for continuous development.

## 5) ANTI-CORRUPTION POLICY

### 1. Principles and Rationale

With the belief in the ideal that conducting business transparently, fairly, and with integrity for all parties, the Company complies with laws and adheres to the Code of Business Ethics that is transparent and auditable, has social responsibility and responsibility to all stakeholder groups according to Good Corporate Governance principles, in order to develop the Company into a Sustainable Organization. The Company has joined as part of the "Thai Private Sector Collective Action Against Corruption" to demonstrate the Company's intent and commitment to oppose corruption in all forms.

The Board of Directors therefore deems it appropriate to establish the "Anti-Corruption Policy" in writing to be used as operational guidelines for the Company's directors, executives, and all employees, or third parties related to the Company to strictly comply with, so that the Company's business operations that may be at risk of fraud and corruption are considered and performed carefully.

### 2. Definitions

Company means Principal Capital Public Company Limited and its subsidiaries and affiliated companies.

Fraud means seeking improper benefits through position or duty, or through the Company's laws, policies, rules, and regulations for one's own benefit or that of others.

Malfeasance means performing or omitting to perform any action in a position or duty, or performing or omitting to perform any action in behavior that may cause others to believe one has a position or duty when one does not have such position or duty, or using authority in a position or duty, in order to seek benefits that should not be properly obtained for oneself or others.

Corruption means bribery, using position or duty and/or using information obtained from performing work duties of the Company to perform any actions that favor oneself, associates, and/or others and government officials, in order to obtain property, any other inappropriate business benefits, or any improper benefits for oneself both directly and indirectly, including any actions that conflict with or contradict the Company's business ethics, except in cases where laws, regulations, notifications, rules, local customs, traditions, or trade practices permit such actions.

Political Contributions means providing financial or in-kind support and/or encouraging employees to participate in political activities in the Company's name to support political parties, politicians, persons related to politics, or political power groups, whether directly or indirectly, leading to disunity and reconciliation within the Company and

the nation, or to obtain special privileges, improper benefits, or business advantages, but does not include employees' participation in activities according to their individual freedom rights.

Sponsorship means money paid to or received from customers, business partners, and business partners reasonably, with the purpose for business, brand, or the Company's reputation, benefits in creating commercial credibility, helping strengthen business relationships, and appropriate to the occasion.

Fraud Risk Management means establishing guidelines and processes for identifying, analyzing, assessing, managing, and monitoring in various work processes of the Company that have opportunities for fraud risk or improper omission of duties, and using analytical results to review measures and establish guidelines to prevent fraud and misconduct, as well as creating transparency in management and operations, to help the Company minimize losses and maximize positive opportunities.

## 3. Policy

(1) The Company's directors, executives, and all employees, or third parties related to the Company are prohibited from committing, accepting, or supporting fraud and corruption in all forms, both directly and indirectly, to persons or related agencies, whether through offering, promising, soliciting, demanding, giving or accepting bribes, or having any behavior suggesting fraud or corruption. Support should be provided to all related organizations, customers, business partners, contractors, and subcontractors to practice similarly to the Company and government officials, and operational guidelines should be reviewed for consistency with policies, regulations, requirements, rules, notifications, laws, and business changes.

(2) The Company has a policy of political neutrality and does not participate in any activities that may cause understanding that the Company is involved in or provides political assistance to any particular political party or power group, by maintaining neutrality without favoring any party or political group, and will not use the Company's assets to support any particular political party or provide assistance to any specific political election candidate. The Company considers that employees can exercise their rights as good citizens according to the constitution and other related laws.

(3) The Company has no policy to give or accept bribes in any form in the Company's business operations. Business operations and dealings with government and private sectors must be transparent, honest, and conducted in accordance with relevant laws.

(4) The Company will control charitable donations, sponsorships, business gifts, and support for various activities to be transparent and in accordance with the law.

(5) The Company establishes appropriate and regular internal controls and audits to prevent all employees, including third parties related to the Company, from acting contrary to this policy.

(6) The Company provides anti-corruption knowledge to the Company's Board of Directors, executives, and all employees, or third parties related to the Company to promote honesty, integrity, and responsibility for duties and responsibilities, as well as communicate the Company's commitment.

## 4. Duties and Responsibilities

4.1 Board of Directors has the following responsibilities:

(1) Establish policies and supervise the establishment of effective systems to support anti-corruption in the Company to ensure everyone in the Company is aware and gives importance to anti-corruption.

(2) Consider reviewing the appropriateness of changes to the anti-corruption policy received from management to be appropriate for the business model, Company environment, and organizational culture.

(3) Have a clear understanding of factors and causes that may result in significant fraud and corruption risks of the Company, along with providing confidence in the methods management uses to manage such risks.

(4) Set an example by demonstrating honesty and commitment to opposing corruption in all forms.

(5) Create and instill an organizational culture of good corporate governance to help prevent and suppress corruption.

(6) Support independent units in performing corruption prevention and suppression work, including the Audit Committee, Risk Management Committee, Internal Auditors, other related Company departments, and external supervisory agencies.

(7) Communicate and emphasize the Board of Directors' and management's commitment to anti-corruption to employees at all levels, including third parties related to the Company, to be aware and take serious action.

4.2 Audit Committee has the following responsibilities:

(1) Review the anti-corruption policy received from management to be appropriate for the business model, Company environment, and organizational culture.

(2) Review the appropriateness of changes to the anti-corruption policy received from management.

(3) Review financial and accounting reporting systems, review internal control audit reports and fraud and corruption risk assessments as proposed by internal auditors to ensure such systems have minimal risk of creating fraud and corruption opportunities affecting the Company's financial position and operating results, and are appropriate for the Company's international standard business model, are comprehensive, appropriate, modern, and effective.

4.3 Risk Management Committee has the following responsibilities:

(1) Consider fraud and corruption risk management policies and frameworks.

(2) (2) Monitor the process of identifying and assessing fraud and corruption risks to report to the Board of Directors regarding risks and risk management.

4.4 Executives have the following responsibilities:

(1) Practice and promote ethics to be an example for employees, including third parties related to the Company, establish systems and provide promotion and support for anti-corruption policies to communicate to employees and all related parties, as well as review the appropriateness of systems and various measures, establish operational procedures to prevent fraud and corruption, such as segregation of duties of operators to provide mutual verification of accuracy and completeness and preparation of supporting documents.

(2) Establish internal controls to prevent fraud and corruption risks in departments and work processes under their responsibility.

(3) Review and monitor employee operations to ensure compliance with the Company's policies, rules, regulations, notifications, and orders.

(4) Report fraud and corruption cases to the Audit Committee or Board of Directors as appropriate on a case-by-case basis.

(5) Promote and create incentives for employees to perform duties with honesty, integrity, and sacrifice for common benefits, honor good people, and oppose fraud and corruption.

(6) Create awareness and communicate channels for reporting fraud and corruption tips to employees.

(7) Promote the Company to have an organizational culture free from fraud and corruption, protect employees who refuse fraud and corruption, such as not demoting, not punishing, or giving negative consequences to employees who refuse fraud and corruption, even if such actions cause the Company to lose business opportunities.

4.5 Employees have the following responsibilities:

(1) Comply with the Company's policies, rules, regulations, and orders related to anti-corruption, as well as ethics and employee ethics.

(2) Report suspicious events or fraud and corruption behavior of the Company's Board of Directors, executives and employees, as well as external persons such as business partners, customers, related parties, etc., according to the process established by the Company.

(3) Support and cooperate in preventing and suppressing fraud and corruption.

(4) Create an organizational culture free from fraud and corruption, as well as appreciate conducting oneself according to moral and ethical principles.

(5) All employees at all levels must disclose conflicts of interest with the Company.

## 5. Guidelines

(1) All employees at all levels must disclose conflicts of interest with the Company. The Company's directors, executives, and all employees must comply with laws, anti-corruption policies, Code of Business Ethics,

Director Code of Conduct, Executive and Employee Code of Conduct, and Good Corporate Governance Policy, as well as the Company's related regulations and operating manuals, as well as any other guidelines the Company may establish in the future.

(2) Company employees must not neglect or ignore when witnessing actions that constitute fraud and corruption related to the Company. They must notify supervisors, responsible persons, or the Audit Committee and cooperate in investigating facts. If in doubt, consult with supervisors or Human Resources and Organizational Development through the Company's various communication channels.

(3) The Company will provide fairness and protection to employees who refuse or report fraud and corruption related to the Company. Employees who refuse or report tips will receive protection without being punished, unfairly transferred, or harassed, including appointing persons to investigate all reported tips.

(4) Those who commit fraud and corruption related to the Company will receive disciplinary penalties according to the Company's work regulations and may receive legal penalties if such actions violate the law.

(5) Giving or receiving sponsorships must be in accordance with Company policy, be correct, transparent, have evidence and accounting records. There will be controls and audits to ensure sponsorships are not fraud and corruption, with approval procedures and use of sponsorships consistent with internal control processes.

(6) The Company will donate for charity in financial or other forms of assistance as part of social contribution activities, as well as for public relations and enhancing the Company's good image, without expecting business results in return.

(7) The Company's charitable donations and sponsorships must be approved by the Company's authorized persons according to the following criteria:

(7.1) Must be activities consistent with and related to the Company's policies and plans.

(7.2) Have specific persons or organizations to receive donations or sponsorships for use clearly.

(7.3) Have clear objectives for using such donations and sponsorships that can be implemented and evaluated.

(7.4) Be activities with defined start and end dates.

(7.5) Clearly specify the location where donations or sponsorships will be used.

(7.6) Must specify the benefits expected to be received from using donations or sponsorships, who will benefit, how they will receive direct and indirect benefits, both quantitatively or qualitatively.

(7.7) Have evidence or receipts specifying money that can verify the use of money and operations.

(7.8) For giving or receiving gifts, entertainment, and expenses, all executives and employees must comply with the Ethics Regarding Giving or Receiving Gifts, Property, or Other Benefits.

### Guidelines: Receiving or Giving Gifts

1) Receiving gifts should be general in nature, not specific, of reasonable value, should not exceed three thousand baht, appropriate to the occasion and season. In cases where employees receive more than one item, employees may choose to receive one item. The remainder will be sent to Human Resources to be raffled to other employees who did not receive.
2) Prohibited from demanding or receiving gifts, property, or any benefits from contractors, subcontractors, customers (both internal customers, meaning employees and other personnel in the Company, and external customers such as insurance companies, construction contractors, etc.), including business partners or those involved in the Company's business operations under any circumstances that may affect decision-making in performing duties.
3) If employees receive gifts from those doing business with the Company valued over 3,000 baht (three thousand baht), whether specified as personal, but necessary to receive to maintain goodwill, friendship, or good personal relationships, the recipient must report to supervisors promptly, and if supervisors deem there is no reason to allow the recipient to retain it for personal benefit, the recipient must submit it to supervisors for such property or benefit to become the Company's property immediately.
4) Do not receive or give gifts of cash, checks, bonds, stocks, gold, gems, real estate, or similar items for personal benefit.
5) Giving gifts or giveaways with a value not exceeding three thousand baht.

## 6. Implementation Requirements

(1) This anti-corruption policy covers the human resource management process from recruitment and selection of personnel, promotions, training and development, employee performance evaluation, and employee compensation, by requiring supervisors at all levels to communicate understanding to subordinates to comply correctly and supervise compliance to be effective.

(2) Any actions according to the anti-corruption policy shall use the guidelines specified in the Code of Business Ethics, Director Code of Conduct, Executive and Employee Code of Conduct, Good Corporate Governance Policy, Internal Controls and Risk Management, Ethics Regarding Giving or Receiving Gifts, Property, or Other Benefits, and other policies and operating procedures that the Company may establish.

## 7. Communication and Disclosure

(1) The Company emphasizes internal communication through various media such as Intranet, bulletin boards, and the Company's human resource management to instill, transfer, and reinforce ethics to employees and executives to create awareness of the importance of good corporate governance, risk management, and internal controls to prevent fraud and corruption, including reporting fraud and corruption to management.

(2) The Company will disclose information to shareholders, executives, customers, employees, stakeholders, and related parties through the Annual Report and the Company's website or any other appropriate methods to ensure the Company conducts business transparently and auditably.

### 8. Management and Risk Assessment

The Company emphasizes the risk management process to identify fraud-related risks in the Company's business operations, such as asset embezzlement, fraud in financial reporting, and other fraud, by considering both the likelihood of occurrence and impact, to find response measures and risk management, consideration of control activities, internal control monitoring processes, including monitoring and evaluating the ability to prevent and detect fraud transactions, errors, and compliance or non-compliance with regulations, to reduce and prevent such risks. Examples of fraud in the Company's various processes include financial fraud, sales, marketing, other services, cash and important documents, as well as procurement, etc.

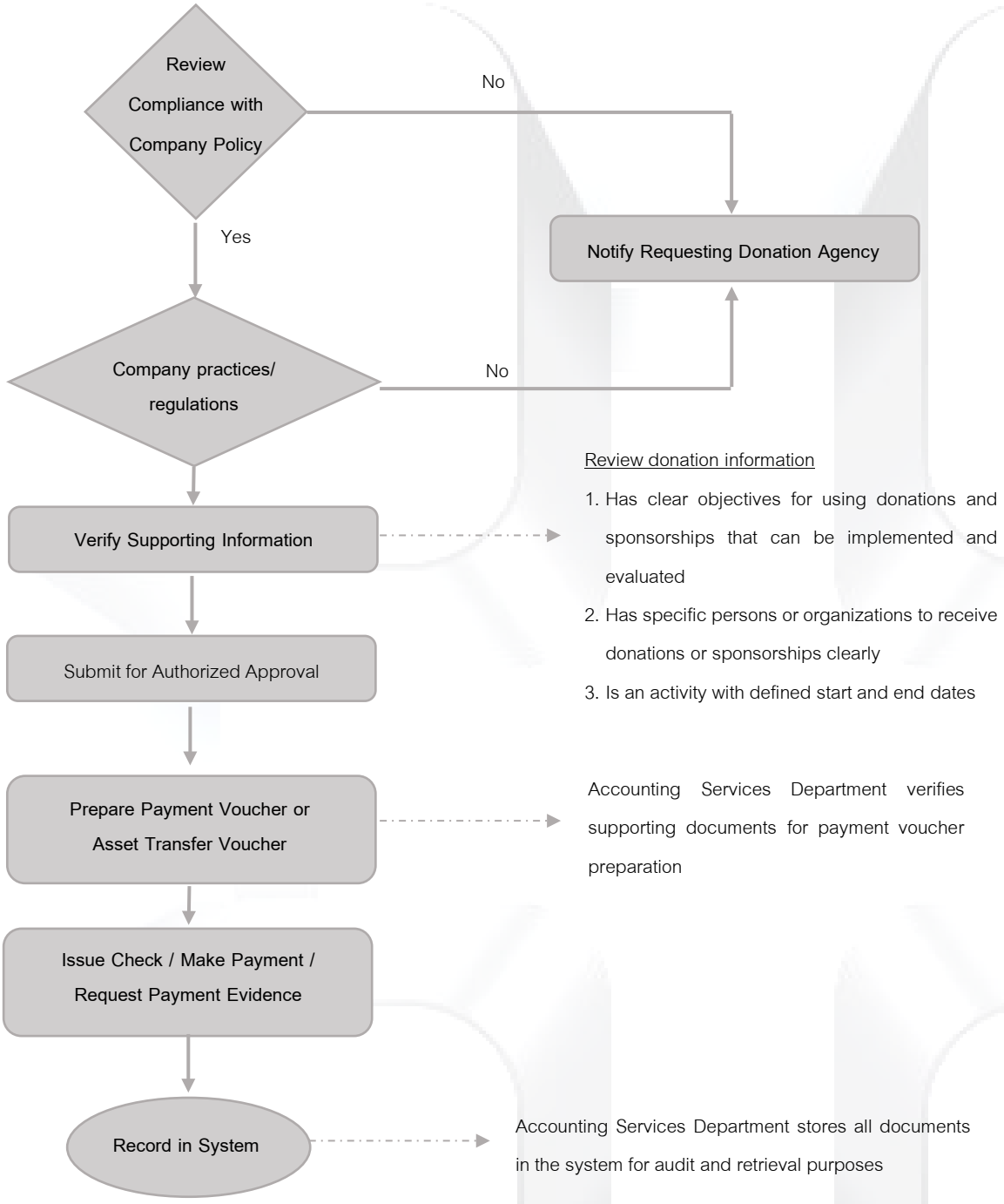
### 9. Monitoring Activities

The Company emphasizes the internal audit process and assessment of adequacy of the internal control system through Self Assessment methods, including supporting the use of technology in continuously and comprehensively auditing fraud and corruption for all transactions.

Internal auditors have duties and responsibilities to audit and review operations to be correct according to policies, guidelines, authority to operate, operating regulations, laws, and requirements of supervisory agencies, to ensure the Company has appropriate and adequate control systems for corruption risks that may occur, and report to the Audit Committee.

## 10. Monitoring Activities

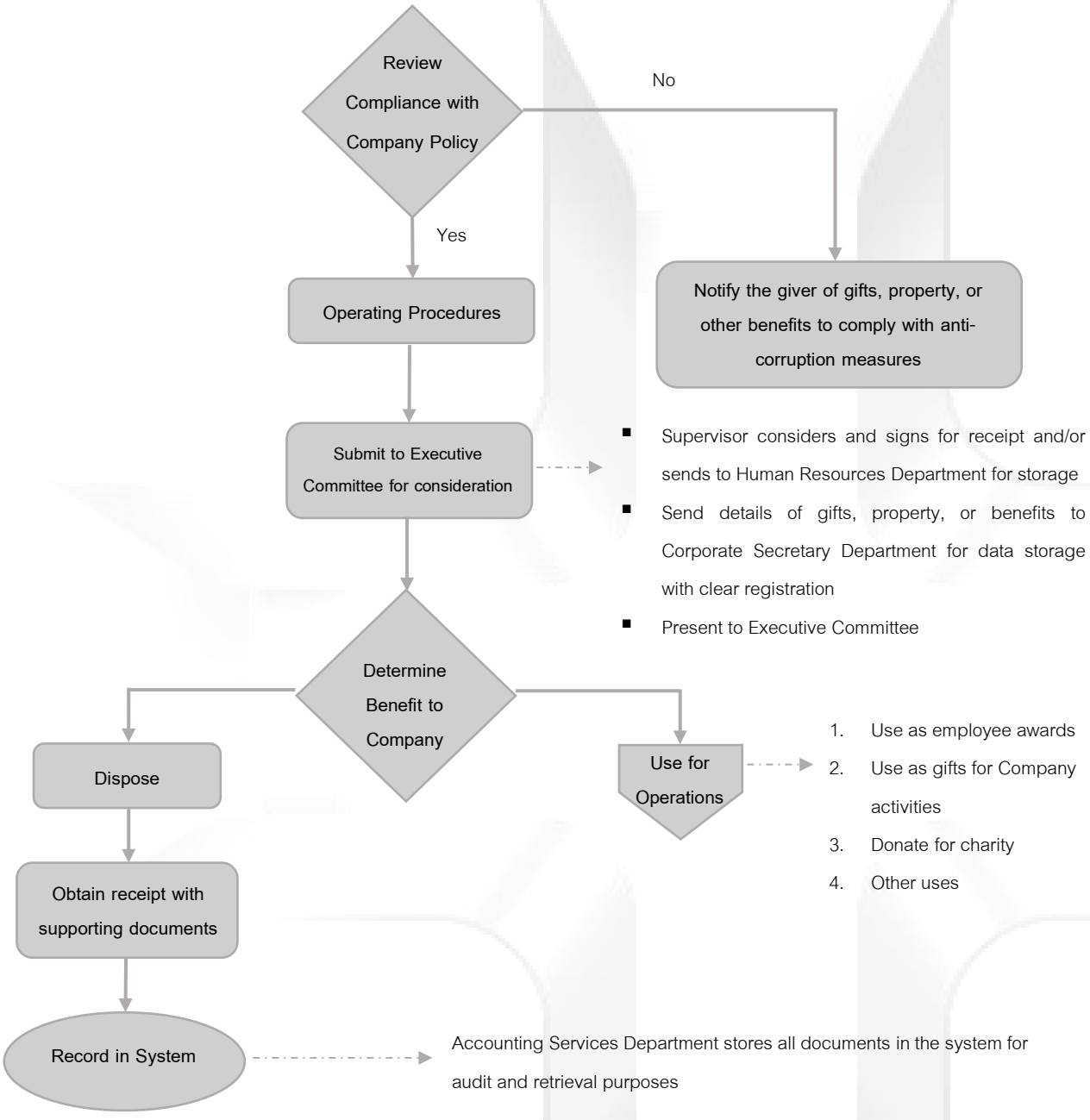
When the Company or any department wishes to make charitable donations and provide sponsorships to any persons or external agencies, in financial or other forms of assistance, as part of social contribution activities, as well as for public relations and enhancing the Company's good image, without expecting business results in return, the procedures are as follows:



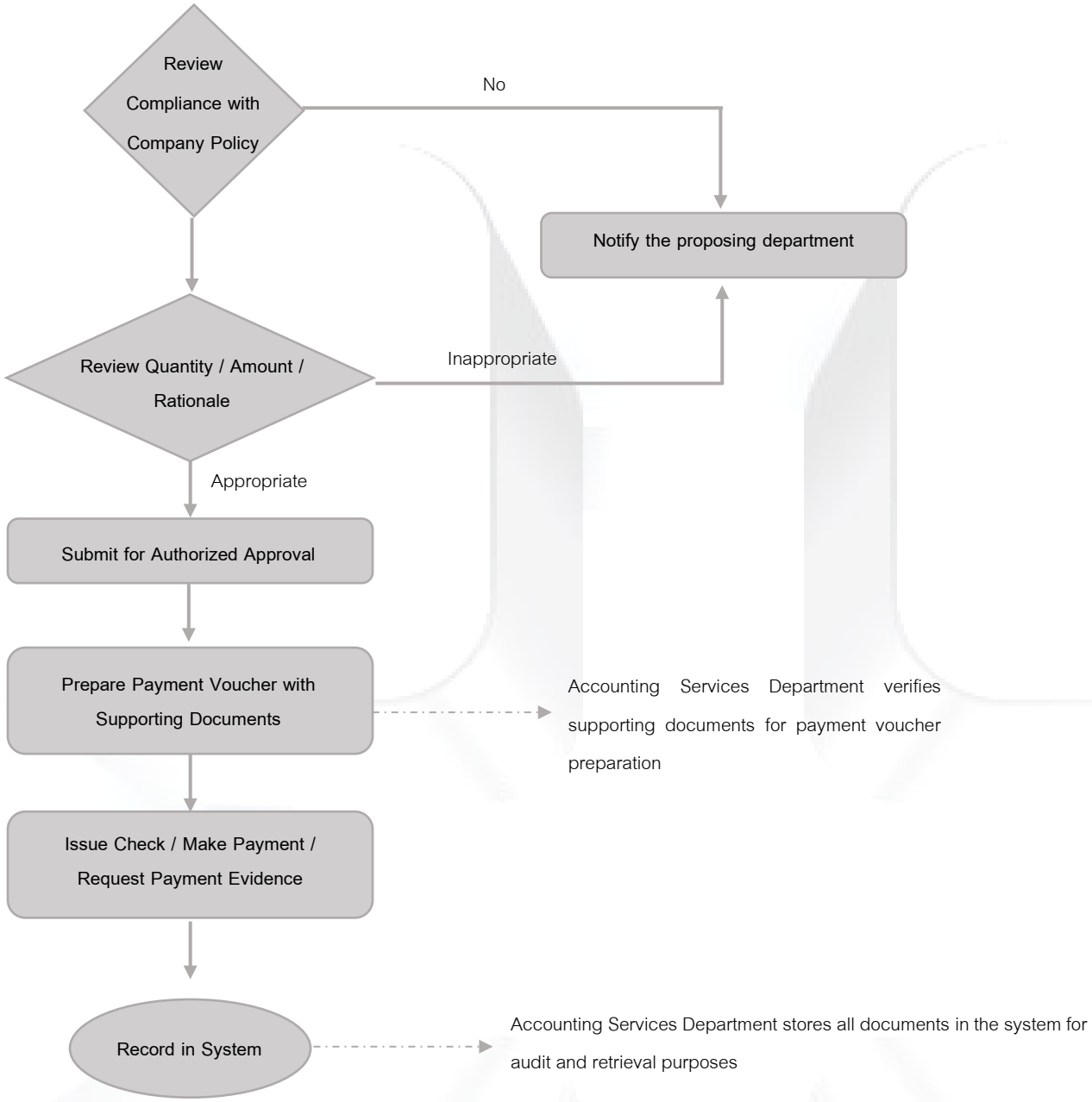
## 11. Procedures for Giving or Receiving Gifts, Property, or Other Benefits and Entertainment

When the Company or any department wishes to give or receive gifts, property, or other benefits to any persons or external agencies in accordance with business customs to maintain good relationships and in compliance with laws, all executives and employees must comply with the Ethics Regarding Giving or Receiving Gifts, Property, or Other Benefits valued over three thousand baht, with the following procedures:

### (1) Receiving Gifts, Property, or Other Benefits and Entertainment



## (2) Giving Gifts, Property, or Other Benefits and Entertainment



## REGULATIONS PROHIBITING BRIBERY OF GOVERNMENT OFFICIALS AND EMPLOYEES

To ensure that the Company's Board of Directors, executives, and employees, as well as third parties, adhere to practices that prevent and eliminate fraud and corruption by prohibiting the offering, payment, promise of payment, or authorization to pay money, gifts, or anything of value to government officials and employees for the following purposes:

- To influence or induce any action or decision from government officials or employees
- To induce any action that violates legal duties
- To obtain inappropriate benefits, or
- To induce government employees to influence other government agencies to act to help obtain or maintain business or for joint business operations

*These regulations are part of the Company's anti-corruption policy.*

### Details of Prohibitions

1. **Prevention of Fraud and Extortion**

Fraud and extortion are criminal offenses. The Company prohibits demanding or ordering, both directly and indirectly, or accepting any benefits through deceptive methods or any other methods to obtain benefits for employees, third parties, subsidiaries, affiliated companies, or for the Company itself.

2. **Bribery**

Offering, paying, demanding, or accepting bribes or under-the-table payments (including facilitation payments) given to or received from any person, whether government or private sector agencies, is strictly prohibited.

All related persons are prohibited from the following matters:

- Giving or offering bribes, under-the-table payments, or similar forms of money or any benefits, whether committed domestically or internationally, to any person or agency (not limited to customers or prospective customers, government officials, government employees, political parties, candidates for political positions, or any intermediaries such as agents, authorized representatives, attorneys, or consultants), and/or
- Accepting or receiving bribes, under-the-table payments, or similar forms of money or any benefits, whether committed domestically or internationally, from any person or agency (not limited to customers or prospective customers, government officials, government employees, political parties, candidates for political positions, or any intermediaries such as agents, authorized representatives, attorneys, or consultants) that were committed intentionally or may be perceived as intended to influence or induce officials to act, omit to act, or make decisions according to what persons, agencies, or the Company desires to:
    - Obtain or maintain business or business benefits of the Company
    - Obtain inappropriate benefits for the Company or any agency for which one is a representative

3. **Facilitation Payments**

The Company strictly prohibits facilitation payments, both directly and indirectly, made for or on behalf of the Company.

Guidelines for Avoiding Facilitation Payments:

- Confirm with officials that the Company must receive receipts as supporting documents for disbursements
- Report matters that are implied, involved, questions, or demands for facilitation payments to supervisors and senior management for acknowledgment, and refuse to make such payments
- Exception situations where one may be threatened, intimidated, or forced to compromise by government officials or employees for one's own safety or security (or that of others) requiring provision or payment. Any payments under such exceptional circumstances must be reported immediately to the Division Manager/Senior Division Manager and senior management. A detailed record of the payment and incident details must be prepared and attached, and this record must be maintained at all times. Additionally, such reports must be presented to the Audit Committee as soon as possible after the incident occurs so that the matter is properly recorded, reviewed, and held accountable by the authorized persons.

4. **Gifts, Entertainment, and Hospitality**

Gifts and Entertainment

All related persons are prohibited from giving or receiving gifts, entertainment, or anything of value to or from persons having business relationships with the Company, except when given or received in compliance with the Company's gift giving and receiving policy.

Before accepting or giving any benefits, appropriateness and legality must be considered under this policy according to established criteria. Generally, the following questions must be answered regarding benefits or advantages to be received:

- Is it genuine?
- Is it appropriate to the circumstances?
- Is it impartial and reasonable?
- Does it not cause the Company discomfort or embarrassment?
- Is it acceptable under laws and customs?
- Does it comply with policies and criteria regarding gifts, entertainment, and hospitality policies (as applicable)?
- Is it not in the form of cash or cash equivalents (such as gift cards/checks or coupons that can be used as cash)?
- Is it given openly, not secretly concealed, and not in a form that appears to avoid improper actions?
- Is it properly documented or certified?
- Is there original receipt evidence, and

- Must it be properly recorded and maintained?

Travel and Hospitality

Special care is specific business hospitality and travel provided to government officials and employees. The Company may pay such expenses or reimburse such expenses to government officials or employees who have paid in advance for reasonable travel and accommodation expenses, including any other directly related expenses for:

- Promoting sales or exhibiting the Company's products and services
- Preparing or signing memoranda of understanding or contracts between the Company and government agencies represented by government officials or employees. Payment or reimbursement of expenses related to travel, entertainment, and accommodation must be permitted under relevant enacted laws and must be approved in advance by the relevant Managing Director or higher only.
- In all cases, the purpose of travel must be clearly specified and approved in advance. Reimbursement of such expenses must be based on "good faith" and must have supporting documentation and be maintained for audit purposes at all times.

Cash payments or daily allowances should be avoided, and disbursement or reimbursement for travel expenses, accommodation, and other related expenses should be paid directly to the government agency, hotel, or store rather than directly to government officials or employees.

In cases where family members of government officials or employees are not invited to travel or participate in organized events but such family members travel with the government officials or employees, the Company will not be responsible for or reimburse any expenses incurred for family members.

5. Donations

Donations must comply with the Company's donation policy. Before making any donations, the Company should ensure that:

- The donation must not be dependent on or made to win business agreements
- The donation is made for regular charitable purposes and is not donated to any specific individual
- Donations should only be made to charitable organizations properly registered according to the laws of the country
- The charitable organization's history must be carefully and thoroughly reviewed to ensure the charitable organization does not act as a source of illegal fundraising that violates or breaches money laundering, terrorism, and other related laws

Charitable donations or such payments must be approved by authorized persons as specified in the Company's authority to operate only. Additionally, such approval authority shall clearly specify the amount that can be approved for donation. For significant donations, approval and consent must be obtained from the Managing Director, and in any case, the charitable or social donation figures must be disclosed before approval every time.

Record Keeping and Accounting Control Requirements

1) Company personnel must provide necessary approval documents consistent with policies and criteria regarding gifts, entertainment, hospitality, and travel.
2) Before any payment is made or approved, Company personnel must ensure that no part of the payment is made for purposes other than those completely and correctly described in the Company's manuals, reports, policies, and records.
3) All gifts, entertainment, or travel provided to government officials or employees must be reported to relevant persons every time.
4) Concealing or not recording the Company's accounts is prohibited for any purpose whatsoever, including prohibiting false or fraudulent record entries in Company reports for any reason whatsoever.
5) Personal funds must not be used to achieve results prohibited by these regulations, gift policies and criteria, or any Company policies and regulations.

Additionally, the Company's Accounting and Finance Department must maintain accounting procedures manuals, financial reports, and controls related to matters covered by these regulations. Internal auditors shall establish internal audit formats to comply with requirements in these regulations. In particular, the Company will supervise and review through verification of compliance with these regulations. Additionally, supervision and review will be conducted by considering the history of Company personnel who have authority to approve Company assets, including persons who must deal with government officials or employees.

## 6) FRAUD AND CORRUPTION RISK MANAGEMENT PROCEDURE

### Principles and Rationale

With the belief in the ideal that conducting business transparently, fairly, and with integrity for all parties, the Company complies with laws and adheres to the Code of Business Ethics that is transparent and auditable, has social responsibility and responsibility to all stakeholder groups according to Good Corporate Governance principles, in order to develop the Company into a Sustainable Organization. The Company has joined as part of the "Thai Private Sector Collective Action Against Corruption" to demonstrate the Company's intent and commitment to oppose fraud and corruption in all forms.

The Board of Directors therefore deems it appropriate to establish the "Fraud and Corruption Risk Management Procedure" in writing with the objectives to:

1) Establish measures or various activities for use in preventing, detecting, and responding to fraud and corruption risks.
2) Clearly identify duties and responsibilities of personnel in each job position in preventing, detecting, and responding to fraud and corruption risks in accordance with good practices.
3) Establish operational guidelines so that Company personnel can prevent, detect, and respond to fraud correctly and timely in cases of suspicion or discovery of actions related to fraud and corruption.

### Scope of the Manual

This Fraud and Corruption Risk Management Procedure is part of the risk management policy and covers operations of directors, executives, and all employees of the Company, or third parties related to the Company.

This Fraud Risk Management Procedure is part of the "Anti-Corruption Policy" approved by the Board of Directors by establishing measures to prevent, detect, and respond to fraud and corruption ("Anti-Corruption Measures") and can be used in conjunction with the "Corporate Governance Policy." Fraud and corruption prevention measures can help the Company reduce risks that may cause fraud and corruption in the organization. Therefore, fraud and corruption risk assessment, design and operation according to appropriate internal controls to reduce fraud and corruption risks, as well as creating awareness and values in opposing fraud and corruption for Company personnel are important factors in helping prevent fraud and corruption in the organization.

The fraud and corruption prevention measures under this Fraud and Corruption Risk Management Procedure consist of five main activities as follows:

### 1. Fraud and Corruption Risk Assessment

Fraud and corruption risk assessment aims to have all departments in the Company proactively identify, assess, and review the organization's fraud and corruption risks, as well as create awareness of fraud and corruption risks that may occur and impacts on the organization's objectives and operations, to ensure fraud and corruption risks are identified and managed timely.

Fraud and corruption risk assessment consists of four main steps:

Step 1: Preparation to establish risk measurement criteria in terms of Impact and Likelihood of Occurrence, as well as establish the Risk Appetite level that the organization accepts.

Step 2: Identifying fraud and corruption risks, root causes of risks, and risk impacts, as well as analyzing severity and likelihood of risk occurrence before considering existing internal control measures.

Step 3: Assessing existing internal control systems, analyzing severity and likelihood of risk occurrence after current internal control measures.

Step 4: Providing measures to reduce risks to acceptable levels if internal control measures currently operating are insufficient to prevent fraud and corruption risks.

## 2. Policies Related to Anti-Corruption

The Company provides policies, operating manuals, and measures to oppose fraud and corruption, such as anti-corruption policy, fraud and corruption risk management procedure, good corporate governance, and business ethics, guidelines for political support and assistance, guidelines for charitable donations and sponsorships, and guidelines for receiving or giving gifts and entertainment, etc., so that Company personnel understand ethical principles and the Company's good operational guidelines, as well as to create awareness and values in opposing fraud and corruption for Company personnel.

All related policies must be approved by the Board of Directors. The Company must regularly review and improve related policies and manuals at least annually to ensure fraud and corruption risks are managed and operational and legal changes are appropriately identified and covered in policies.

## 3. Communication and Training

Communication and training are necessary in fraud and corruption prevention measures to create knowledge, understanding, and awareness of the importance of complying with policies and manuals related to anti-corruption, as well as various anti-corruption measures to promote participation in the organization's fraud and corruption risk management, as well as enable Company personnel to be part of helping prevent and detect fraud and corruption in the organization, as well as communicate to business stakeholders to demonstrate commitment to anti-corruption and transparency in Company operations.

Therefore, the Human Resources Department must prepare an annual written communication plan for anti-corruption policies and measures for Company personnel and business stakeholders, as well as establish communication channels such as Company bulletin boards, training, public relations through the Company's Intranet system, and the Company's website, etc., appropriate for both internal and external message recipients. Such work plans and communication channels must be reviewed and approved by the Managing Director annually. Additionally, to ensure communication effectiveness, established work plans and communication channels should be reviewed and internal control systems assessed by the Internal Audit Department to ensure activities organized are sufficient and can create awareness for all Company personnel and business stakeholders.

## 4. Background Review of Personnel and Business Stakeholders

Background review of personnel and business stakeholders is an important factor making fraud prevention effective. The Company assigns the Human Resources Department to review personnel backgrounds before hiring and promotions, and the Procurement Department to review business stakeholder backgrounds before starting contracts or transactions.

Background reviews can be conducted appropriately under relevant laws and with consent from personnel or business stakeholders as follows:

- Review personnel backgrounds before hiring to verify qualifications, appropriateness, and experience of job applicants
- Review personnel backgrounds before assigning to hold important positions within the Company, such as Board of Directors, senior executives, personnel in finance departments, etc., to verify qualifications, experience, financial credibility, references, or conflicts of interest that may arise from holding new positions
- Review backgrounds of business stakeholders, especially vendors, contractors, and service providers to the Company, to verify credibility, financial status, reputation, and qualifications related to products or services of business stakeholders

Additionally, the Board of Directors, executives, and personnel holding important positions as determined by the Human Resources Department, as well as business stakeholders, must report conflicts of interest that may occur to the Managing Director and Board of Directors annually and during the year if there are any changes that may cause conflicts of interest. The Company prohibits personnel with conflicts of interest from being involved in procurement processes and will punish personnel who do not report conflicts of interest timely.

## 5. Internal Controls

Internal controls are operational processes jointly established by the Board of Directors, executives, and organizational personnel at all levels to provide reasonable assurance that methods or operations as specified will help the organization achieve objectives. Therefore, internal controls are the Company's primary tools for preventing fraud and corruption in operational processes of all departments. Executives in each department must design appropriate internal controls for processes under their responsibility to manage and reduce fraud and corruption risks jointly identified in fraud and corruption risk assessment to acceptable organizational levels, as well as communicate understanding and control and monitor operations of personnel in departments to operate according to established internal control systems.

All departments must prepare written operational procedures or processes for all processes for executives to review and approve for enforcement, considering clear segregation of duties in assigning personnel duties in operations according to procedures or operational processes so that operations are transparent, independent, and can help prevent or detect fraud and corruption risks, as well as store such documents in channels that related personnel can access and communicate to related personnel for acknowledgment.

### Fraud and Corruption Detection Measures

Good fraud and corruption prevention measures can help reduce the likelihood of fraud and corruption to some extent. However, the Company needs to establish fraud and corruption detection measures to help detect

and report actions that may be fraud and corruption timely. Therefore, whistleblowing mechanisms and fraud and corruption reporting are main activities that can help the Company detect fraud and corruption. Additionally, to ensure fraud and corruption detection measures are appropriate, efficient, and effective, the Internal Audit Department must review the design and internal controls of such measures annually. Fraud and corruption detection measures consist of two main activities:

### 1. Whistleblowing Mechanisms

Management establishes reliable and independent channels for reporting tips about fraud and corruption, including providing opportunities for everyone, whether Company personnel or external persons, to report tips without revealing identity, as well as establishing whistleblower protection processes to protect reporters from being harmed or threatened afterward, which helps encourage Company personnel to have confidence and feel safe in reporting incidents or tips about fraud and corruption.

Company personnel therefore have a duty to report incidents or tips of fraud and corruption through channels established by the Company. The Company will punish Company personnel who know or have information about events that may be fraud but do not notify responsible persons, whereby the Company has measures to protect those who report incidents or tips in good faith truthfully. However, the Company will punish those who intentionally report incidents or tips that are untrue.

Currently, the Company establishes multiple complaint channels. External persons can submit complaints or suggestions through various channels as follows:

1. External cases, contact Company Secretary

   Website : Contact us at www.principalcapital.co.th

   Telephone : 02-009-2015

   Email : Princ_secretarywhistle@princgroup.com

   Mail : Company Secretary
   Principal Capital Public Company Limited
   29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63,
   Khlong Tan Nuea, Watthana, Bangkok 10110

2. Employee cases, contact Whistleblowing Committee (Internal)

   Email : Princ_internalwhistle@princgroup.com

   Mail : คณะกรรมการรับแจ้งเบาะแส (ภายใน)
   29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63,
   Khlong Tan Nuea, Watthana, Bangkok 10110

The terms and procedures for considering tips and complaints are specified in the "Corporate Governance Policy" and the Company's website, which Company personnel and external persons can access.

### 2. Fraud and Corruption Reporting

When fraud and corruption incidents or tips are reported, the Company Secretary collects data from tip reports and other information related to fraud and corruption, such as the number of fraud and corruption tip reports, event summaries and operational status, cases of fraud occurring in operational status according to anti-corruption measures, etc., to report to the Executive Committee monthly and to the Board of Directors and Audit Committee quarterly. In cases where reported tips are severe and need urgent correction, the Company Secretary must report such fraud events to the Board of Directors, Audit Committee, and related personnel immediately.

All information in reports must be kept confidential. The Company Secretary must report directly only to authorized persons as specified. Sharing information in any form whatsoever to unrelated departments or persons is prohibited.

## Fraud and Corruption Response Measures

The Company establishes fraud and corruption response measures to correct and remedy impacts from fraud occurrence, as well as find ways to prevent fraud and corruption of the same type from occurring again. Fraud and corruption response measures consist of internal investigation, punishment and remediation, and information disclosure.

### 1. Investigation

When fraud occurs, the Company assigns the Managing Director to consider tip information and has authority to approve starting investigation when seeing that obtained tips are sufficient and substantiated, and appoint an Investigation Committee.

In the investigation process, the Investigation Committee must operate with fairness and not disclose information to unrelated persons, including regularly reporting progress or investigation results to the Managing Director monthly for use in reporting to the Executive Committee. In cases where the Investigation Committee encounters obstacles in operations that may affect the Company, the Investigation Committee must report to the Managing Director to report such matters to the Board of Directors or Audit Committee for urgent solutions.

Additionally, the Investigation Committee must record investigations and store both physical and electronic evidence for at least 3 years or until the statute of limitations expires to ensure the Company has sufficient evidence if needed for use in court.

### 2. Punishment and Remediation

Strict and decisive punishment demonstrates the Company's position on fraud and corruption to both employees and stakeholders, while remediation of impacts from fraud and corruption is something the Company must prioritize and implement timely to demonstrate attention and commitment to solving fraud and corruption issues.

#### 2.1 Punishment

When investigation is complete and fraud and corruption are found to have actually occurred, the Investigation Committee has a duty to present facts and evidence to authorized persons to consider punishment consistent with Company policies and other related laws.

The Company stipulates that the home department of the fraudster is responsible for punishment by referring to "Employee Disciplinary Investigation" and "Employee Code of Conduct, Standards of Conduct, and Actions Constituting Company Disciplinary Offenses" for punishment procedures and those with authority to punish, which must record punishment consideration methods and punishment conclusions and must be stored with important documents in investigation procedures for at least 3 years. Additionally, in cases where punishment creates legal risks for the Company, Investigation Committee representatives must consult with the Legal Department and management clearly before proceeding.

### 2.2 Remediation

When investigation is complete, management must jointly consider remediation measures from fraud events that occurred, such as improving or adding Company policies, improving or adding internal controls, changing operational methods, filing criminal and/or civil lawsuits, extending investigation results to examine fraud and corruption in other parts that may be related, etc., by assigning duties to related departments. For remediation measures in each case, prepare a remediation action plan with operational timeframes to present to the Managing Director and implement according to approved remediation plans.

The Company stipulates that the Chairman of the Board or personnel assigned by the Chairman of the Board disclose important information about fraud and corruption to external supervisory agencies (such as the Securities and Exchange Commission, the Stock Exchange of Thailand, etc., or to the public). However, the Company stipulates those decisions to disclose information related to fraud and corruption in each topic depend on the Chairman of the Board's discretion.

The Company prohibits those without duties or not assigned by the Chairman of the Board from disclosing fraud information to other persons in the Company, mass media, or any agencies whatsoever. Additionally, the Company will consider punishing violators without exception.

This Fraud and Corruption Risk Management Procedure is part of the risk management policy and is under supervision of the Audit Committee. This manual will be reviewed and improved annually or when there are significant changes affecting fraud and corruption risk management, to ensure the manual is consistent with Company practices and complies with regulations and other related laws.

APPENDIX

Company Internal Operational Processes with Corruption Risks in Both Private Sector and Government Agencies

| No. | Company Operational Processes Related to Government and Private Agencies with Corruption Risk | Name of Government and/or Private Agency Contacted | Name of Company Internal Department | Number of Contacts/Year | Risk Level |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

## 7) INTERNAL WHISTLEBLOWING POLICY

The Company has established the Internal Whistleblowing Policy to enable internal personnel to report complaints or tips in cases where fraud, corruption may occur, or witness suspicious actions that violate or fail to comply with laws, regulations, rules, ethics, or the Company's corporate governance policy, to help improve, correct, or take action to ensure correctness, appropriateness, transparency, and efficiency in sustainable business operations.

**Objectives**

1.1 To encourage internal personnel to be aware of and prioritize abnormal events within the organization and be able to report complaints or tips immediately if witnessing misconduct or suspicious behavior suspected of wrongdoing from improper practices not in accordance with relevant laws or regulations, fraud and corruption, as well as non-compliance with the Company's corporate governance policy and business ethics.

1.2 To ensure the Company's operations are correct, appropriate, transparent, and more efficient in accordance with good corporate governance principles and prevent risks of damage that may occur.

1.3 To emphasize the importance of the whistleblowing process and to protect honest complainants, whereby whistleblower information and reported matters will be kept confidential without disclosure to others.

In cases where employees and various stakeholder groups have doubts or witness actions suspected of violating or failing to comply with laws, regulations, rules, ethics, or corporate governance policy, they can inquire, report tips, or complain and send details and various evidence to relevant persons or departments by contacting as follows:

**Whistleblowing Channels**

Website : Princ_internalwhistle@princgroup.com

Mail : Whistleblowing Committee (Internal)
29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63,
Khlong Tan Nuea, Watthana, Bangkok 10110

**Conditions and Consideration of Tips and Complaints**

1. Details of tips or complaints must be truthful, clear, or sufficient to investigate facts for further action, and whistleblowing should be raised with good intentions, not for personal benefit.
2. The Whistleblowing Committee and assignees will keep received information and related information confidential without disclosing the name of the whistleblower or complainant to the public without consent, and primarily consider the safety and damage to the whistleblower or those who cooperate in information verification.
3. Whistleblowers can choose not to disclose their name, address, or contact telephone number if they believe disclosure will cause insecurity or any damage. However, if they reveal themselves, it will enable reporting of progress, inquiry for additional useful information, clarification of facts, or damage mitigation more conveniently and quickly.
4. The timeframe for handling complaints depends on the complexity of the matter, the sufficiency of documentary evidence received from the complainant, including documentary evidence and explanations from the accused.
5. In cases where whistleblowers or those who cooperate in fact verification believe they may receive insecurity or may experience hardship or damage, whistleblowers or those who cooperate in fact verification may request the Company to establish appropriate protection measures, or the Company may establish protection measures without the whistleblower or those who cooperate in fact verification having to request if it is deemed likely to cause hardship, damage, or insecurity.
6. In cases where whistleblowers or those who cooperate in fact verification experience hardship or damage, the Company will mitigate damage through appropriate and fair processes.

**Operational Guidelines**

1. Whistleblowers can report misconduct according to Section 1.1 in writing with signature and send to the Whistleblowing Committee through whistleblowing channels according to Sections 1) and 2).
2. The Whistleblowing Committee must keep all information confidential without disclosing information to others and will notify the whistleblower after receiving the matter within 2 working days to confirm receipt of whistleblowing information, only in cases where the whistleblower discloses informant information.

3. The Whistleblowing Committee verifies whistleblowing information whether it is likely that misconduct occurred or there is suspicious behavior suspected of wrongdoing according to Section 1.1.
    3.1 In cases where allegations do not fall under or are not sufficiently suspicious to constitute fraud or corruption and there is no need for further investigation, the Chief Internal Audit Executive will report the whistleblowing to senior management. If senior management has no doubts, the Chief Internal Audit Executive must notify the whistleblower why there is no investigation, in cases where the whistleblower discloses informant information.
    3.2 In cases where allegations fall under or are sufficiently suspicious to constitute fraud or corruption and investigation is necessary, the Chief Internal Audit Executive shall report to senior management to request establishment of an Investigation Committee to find facts or recommend appropriate corrective methods or disciplinary action as deemed appropriate.
4. The Chief Internal Audit Executive prepares a summary report of facts to present to senior management and the Audit Committee at least once per quarter.
5. When investigation concludes, the Chief Internal Audit Executive will notify the whistleblower of such investigation results, in cases where the whistleblower discloses informant information.
    5.1 Whistleblowing information and all related documents will be kept confidential by the Whistleblowing Committee with a retention period for information and documents of not less than 5 years.

**Whistleblower Protection Measures**

Whistleblowers acting in good faith will receive appropriate protection. The Company will keep information and identity of whistleblowers confidential. If the Company needs to disclose information, the Company will disclose only necessary information, considering the safety and damage to whistleblowers. The Company establishes complainant protection measures according to the following criteria:

1. Assignees will keep related information confidential without disclosing the name of the whistleblower or complainant to the public without consent, and consider the safety and damage to reporters or those who cooperate in information verification.
2. Received information will be considered confidential. The timeframe for handling complaints depends on the complexity of the matter, the sufficiency of documentary evidence received from the complainant, including documentary evidence and explanations from the accused.
3. Whistleblowers or complainants can choose not to disclose their name, address, or contact telephone number if they believe disclosure will cause insecurity or any damage. However, if they reveal themselves, it will enable reporting of progress, inquiry for additional useful information, clarification of facts, or damage mitigation more conveniently and quickly.

4. Whistleblowers or complainants will receive rights protection, whether Company employees or external persons.

**False Whistleblowing**

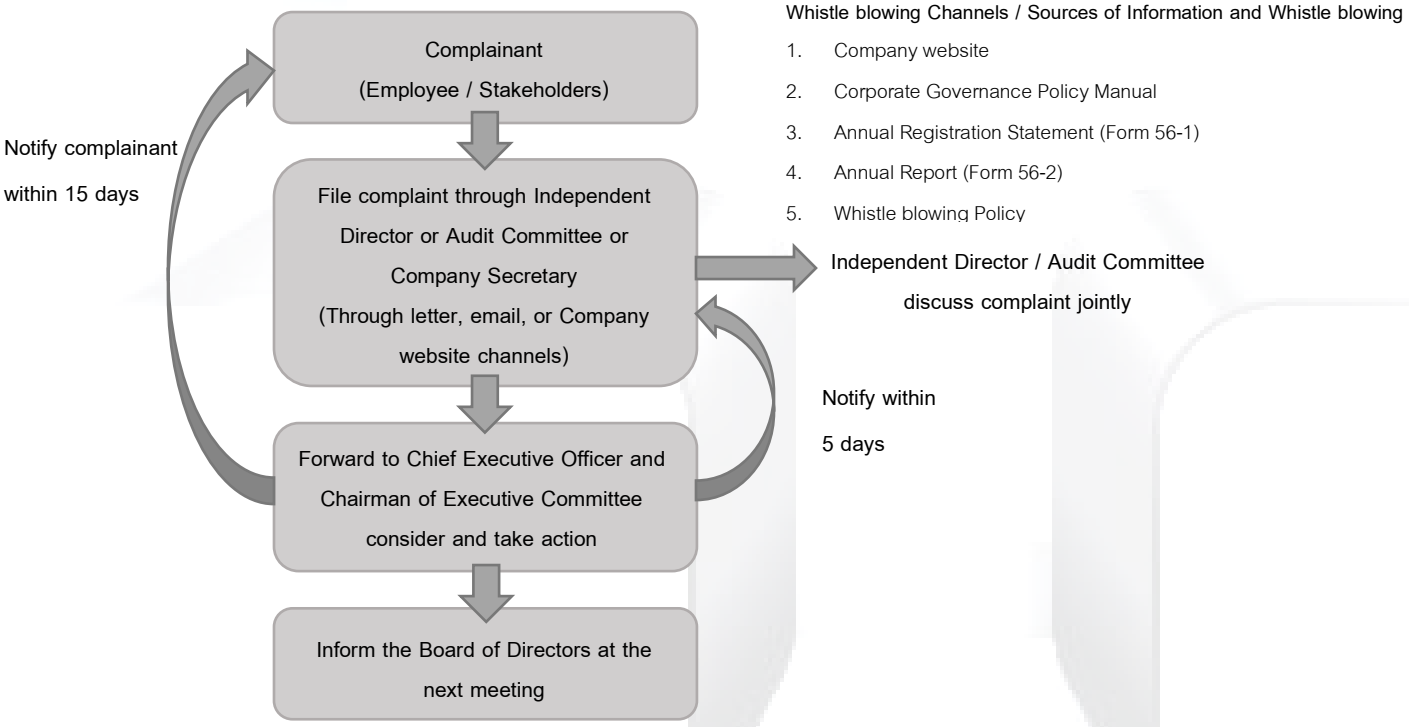
Whistleblowers are aware and understand well that whistleblowing must be done honestly, without intention to harass the organization or individuals, or with dishonest or unfair intentions. If whistleblowers provide false information, the Company will proceed according to Company procedures or Company regulations or relevant laws regarding whistleblowers as appropriate on a case-by-case basis.

**Protection of Rights of Employees, Workers, or Other Persons Employed by the Company**

The Company will guarantee that it will not be a reason or be considered a reason to change job position, nature of work, or workplace, suspend from work, threaten, interfere with work performance, terminate employment, punish, or take any action causing adverse effects when:

a. Providing information, cooperation, or assistance in any manner whatsoever to the Board of Directors, executives, government agencies, or regulatory agencies in cases where such persons have reasonable cause to believe in good faith that there is a violation or non-compliance with laws, regulations, rules, ethics, or corporate governance policy.

b. b. Giving testimony, submitting documentary evidence, or providing assistance in any manner whatsoever to the Board of Directors, executives, government agencies, or regulatory agencies for the benefit of consideration or inspection in cases of suspicion that there is a violation or non-compliance with laws, regulations, ethics, or corporate governance policy.



## 8) RELATED PARTY TRANSACTION POLICY

To ensure transparency and fairness to all shareholders equally, as well as good corporate governance, the Company has established the "Related Party Transaction Policy" based on the following principles:

- Transactions that go through transparent approval processes by directors and executives with responsibility, prudence, honesty, and integrity, whereby stakeholders do not participate in decision-making
- Transactions conducted considering the Company's interests as if conducting transactions with external parties
- Having monitoring and inspection systems that ensure transactions are conducted according to correct procedures

Definitions

According to Capital Market Supervisory Board Notification No. TorJor. 21/2008 regarding Criteria for Related Party Transactions, requiring listed companies to comply with criteria established by the Stock Exchange, the Company has defined terms according to the aforementioned SEC notification as follows:

**"Related Party Transactions"** means transactions between the Company or subsidiaries (the Company holds more than 50 percent of all voting shares, including companies held in successive tiers starting from subsidiaries where the Company holds more than 50 percent first) with related parties of the Company, or transactions between subsidiaries and related parties of subsidiaries.

**" Agreement to Enter into Transaction"** means entering into or agreeing to enter into a contract or any agreement, whether directly or indirectly, to cause acquisition or disposal of assets, leasing or renting assets, providing or receiving services, providing or receiving financial assistance, and issuing new securities, including creating rights or waiving rights to such actions.

**"Related Parties"** means persons who may cause directors or executives of the Company to have conflicts of interest in deciding whether to consider the interests of such persons or the Company's best interests as paramount, including:

(1) Directors, executives, major shareholders, controlling persons, or persons to be proposed as directors, executives, or controlling persons of the Company or subsidiaries, including related persons and close relatives of such persons.

(2) Any juristic person having major shareholders or controlling persons as the following persons of the Company or subsidiaries:

  (a) Directors

  (b) Executives

  (c) Major shareholders

  (d) Controlling persons

  (e) Persons to be proposed as directors, executives, or controlling persons

  (f) Related persons and close relatives of persons under (a) through (e)

(3) Any person who by circumstances can be indicated as acting on behalf of or under the influence of persons under (1) through (2) affecting decision-making, policy determination, management, or operations significantly, or other persons the Stock Exchange deems to have similar circumstances.

(4) Directors of juristic persons having control over the Company's business.

(5) Spouses, children, or adopted children who have not reached legal age of directors under (4).

(6) Juristic persons controlled by persons under (4) or (5).

(7) Any person who acts with understanding or agreement that if the Company conducts transactions providing financial benefits to such persons, the following persons will receive financial benefits:

(7.1) Directors of the Company

(7.2) Executives of the Company

(7.3) Persons having control over the Company's business

(7.4) Directors of persons having control over the Company's business

(7.5) Spouses, children, or adopted children who have not reached legal age of persons under (7.1) through (7.4)

**"Executives"** means directors, managing directors, or persons holding the first four (4) executive positions below the managing director, persons holding positions equivalent to the fourth (4) executive level, and includes persons holding executive positions in accounting or finance lines at the division director level or higher or equivalent.

**"Major Shareholders"** means shareholders, whether directly or indirectly in the Company, exceeding 10 percent of voting shares of the Company, including shares held by related persons and close relatives.

**"Related Persons"** means persons or partnerships under Section 258 (1) through (7) of the Securities and Exchange Act B.E. 2535 (original version), including:

(1) Children who have not reached legal age

(2) Spouses

(3) Ordinary partnerships where such persons, including (1) through (2), are partners

(4) Limited partnerships where such persons, including (1) through (2), are unlimited liability or limited liability partners totaling more than 30%

(5) Limited companies or public limited companies where such persons, including (1) or (2) or (3) or (4), hold shares totaling more than 30%

(6) Limited companies or public limited companies where such persons, including (1) or (2) or (3) or (4) or (5), hold shares totaling more than 30%

(7) Juristic persons under Sections 246 and 247 (under the Securities and Exchange Act) having management authority as representatives of juristic persons

**"Close Relatives"** means persons having blood relationships or by legal registration, including:

(1) Spouses

(2) Fathers, mothers

(3) Siblings

(4) Children and spouses of children

**"Controlling Persons"** means persons having control over business, namely:

(1) Shareholders having voting rights in the Company exceeding 50 percent of all voting rights of the Company

(2) Persons controlling majority votes at the Company's shareholders' meeting, whether directly or indirectly, or for any other reason

(3) Controlling appointment or removal of at least half of all directors, whether directly or indirectly

(4) Other persons who by circumstances have influence over policy determination, management, or operations of the Company significantly, whether such influence derives from being a shareholder or receiving authority by contract or otherwise

**"Normal Trading Conditions"** means trading conditions having fair prices and terms that do not cause transfer of benefits, including trading conditions having prices and terms as follows:

(1) Prices and terms the Company or subsidiaries receive from or give to general persons

(2) Prices and terms related parties give to general persons

(3) Prices and terms the Company can demonstrate are prices and terms business operators of similar nature give to general persons

**"Normal Business Transactions"** means trading transactions the Company or subsidiaries normally conduct to operate business.

**"Transactions Supporting Normal Business"** means trading transactions the Company or subsidiaries conduct to support the Company's normal business transactions.

Characteristics of Related Party Transactions can be divided into 2 characteristics as follows:

(1) When the Company or subsidiaries conduct transactions with:

(a) Executives

(b) Major shareholders

(c) Related persons or close relatives of executives or major shareholders

(2) When the Company or subsidiaries conduct transactions with other companies having major shareholders or controlling persons as executives, major shareholders, controlling persons, or persons to be proposed as executives or controlling persons of the Company or subsidiaries, including related persons or close relatives of such persons.

**Types of Related Party Transactions** The Stock Exchange of Thailand Board Notification has 5 types in total:

(1) Normal business transactions

(2) Transactions supporting normal business

(3) Real estate leasing or rental transactions not exceeding 3 years

(4) Transactions related to assets or services

(5) Financial assistance giving or receiving transactions

STOCK EXCHANGE OF THAILAND BOARD NOTIFICATION TABLE: Information Disclosure and Operations of Listed Companies in Related Party Transactions

| Type of Related Party Transaction | Transaction Value | Disclose to SET | Board of Directors Approval | Shareholder Meeting Approval |
|---|---|---|---|---|
| 1. Normal Business Transactions or Transactions Supporting Normal Business<br>1.1 Normal business transactions with normal trading conditions<br>1.2 Transactions supporting normal business with normal trading conditions and compensation can be calculated from assets or reference value | | - | - | - |
| 1.3 Transactions supporting normal business with normal trading conditions and compensation cannot be calculated from assets or reference value | ≤ 1 million baht or ≤ 0.03% of net tangible assets, whichever is higher | - | - | - |
| | > 1 million baht but < 20 milliom baht or > 0.03% but < 3% of net tangible assets, whichever is higher | ✓ | - | - |
| | ≥ 20 million baht or ≥ 3% of net tangible assets, whichever is higher | ✓ | ✓ | - |
| 1.4 Normal business transactions or transactions supporting normal business without normal trading conditions | ≤ 1 million baht or ≤ 0.03% of net tangible assets, whichever is higher | - | - | - |
| | > 1 million baht but < 20 million baht or > 0.03% but < 3% of net tangible assets, whichever is higher | ✓ | ✓ | - |
| | ≥ 20 million baht or ≥ 3% of net tangible assets, whichever is higher | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| **2. Real Estate Leasing or Rental Transactions Not Exceeding 3 Years and Cannot Demonstrate Normal Trading Conditions** | ≤ 1 million baht or ≤ 0.03% of net tangible assets, whichever is higher | - | - | - |
| | > 1 million baht but < 20 million baht or > 0.03% but < 3% of net tangible assets, whichever is higher | ✓ | - | - |
| | ≥ 20 million baht or ≥ 3% of net tangible assets, whichever is higher | ✓ | ✓ | - |
| **3. Transactions Related to Assets or Services** | ≤ 1 million baht or ≤ 0.03% of net tangible assets, whichever is higher | - | - | - |
| | > 1 million baht but < 20 million baht or > 0.03% but < 3% of net tangible assets, whichever is higher | ✓ | ✓ | - |
| | ≥ 20 million baht or ≥ 3% of net tangible assets, whichever is higher | ✓ | ✓ | ✓ |
| **4. Financial Assistance Giving or Receiving Transactions**<br>4.1 The Company or subsidiaries provide financial assistance to related parties as follows:<br>• Related parties who are natural persons | < 100 million baht or < 3% of net tangible assets, whichever is lower | ✓ | ✓ | - |
| • Related parties who are juristic persons where the Company or subsidiaries hold shares in a proportion less than the proportion held by other related parties who are not the Company or subsidiaries, as the case may be, in such juristic person | ≥ 100 million baht or ≥ 3% of net tangible assets, whichever is lower | ✓ | ✓ | ✓** |

| | | | | |
|---|---|---|---|---|
| ** In cases where the Company or subsidiaries and related parties jointly provide financial assistance to a juristic person where the Company or subsidiaries and related parties are shareholders according to their proportionate interests in such juristic person under normal trading conditions or better, the Company will be exempted from requesting shareholder meeting approval for such transactions. | | | | |
| 4.2 Other financial assistance giving or receiving transactions besides 4.1 | ≤ 1 million baht or ≤ 0.03% ของมูลค่าสินทรัพย์ที่มีตัวตนสุทธิแล้วแต่จำนวนใดจะสูงกว่า | - | - | - |
| ** In cases where the Company or subsidiaries and related parties jointly provide financial assistance to a juristic person where the Company or subsidiaries and related parties are shareholders according to their proportionate interests in such juristic person under normal trading conditions or better, the Company will be exempted from requesting shareholder meeting approval for such transactions. | > 1 million baht but < 20 million baht or > 0.03% but < 3% of net tangible assets, whichever is higher | ✓ | ✓ | - |
| | ≥ 20 million baht or ≥ 3% of net tangible assets, whichever is higher | ✓ | ✓ | ✓** |

This table is announced by the Stock Exchange of Thailand Board regarding Information Disclosure and Operations of Listed Companies in Related Party Transactions (No. 2) B.E. 2004, dated July 21, 2004.

Legend: ✓ means the Company is required to take action according to the column heading marked "✓"

- means the Company is not required to take action according to the column heading marked "-"

## OPERATIONAL GUIDELINES FOR RELATED PARTY TRANSACTIONS

### 1. Prevention of Conflicts of Interest

The Company emphasizes transparent consideration of various transactions that are beneficial and important. Therefore, the Company emphasizes prevention of transactions that may constitute conflicts of interest, related party transactions, or inter-company transactions with the following important principles:

1. Directors and executives must notify the Company Secretary immediately when related party transactions occur in business that may cause conflicts of interest.
2. The Company Secretary has the following duties:
   2.1 Prepare summary reports compiling relationships of the Company's directors and executives, notify various departments, the Managing Director, Executive Committee, Risk Management Committee, Audit

Committee, and Board of Directors for use as information in considering whether to enter into transactions that are related party transactions.

2.2 Review the currency (Update) of information on positions held and shareholdings of directors and executives quarterly: January, April, June, and September.

2.3 Consider related party transactions regarding transactions that occur, authorized persons to approve must be at the appropriate level according to approval procedures, including coordinating with transaction owners to prepare supporting documents to present to the Audit Committee meeting, Board of Directors meeting, and shareholders for consideration in sequence.

3. Procurement Department, departments entering into employment contracts such as Human Resources Department, Project Engineering Department, Building Management Department must verify names of business partners and contracting parties whether they are related parties according to the report in Section 2.1. If yes, must submit through the Company Secretary to consider related party transactions regarding transactions that occur and what level of authorized persons must be proposed according to inter-company transaction or related party transaction approval procedures.
4. Central Accounting Department must verify documents and contracts for procurement, employment, leasing or renting, lending or borrowing money immediately upon receipt from various departments to verify whether they are related party transactions. If yes, must notify the Managing Director and submit through the Company Secretary to consider related party transactions regarding transactions that occur and what level of authorized persons must be proposed according to inter-company transaction or related party transaction approval procedures.
5. Risk Management Committee assesses risks according to related party transaction policies of all departments.
6. Executives and employees must comply with the Company's regulations and business ethics, which are important matters that must be strictly adhered to, so that the Company is trusted and relied upon by all stakeholders, and provide dissemination of information and understanding of employee compliance throughout the Company.

## 2. Procedures for Inter-Company Transactions or Related Party Transactions

The Company has established procedures for related party transactions as follows:

1. All departments must consider whether transactions are related party transactions with the Company by using the same criteria as normal trading and verify with summary reports compiling relationships of the Company's directors and executives prepared by the Company Secretary.
2. All departments must consider comparing prices of products or services with external prices under identical or similar conditions.

3. All departments may utilize reports from independent appraisers appointed by the Company or group companies to make price comparisons for significant inter-company transactions to ensure such prices are reasonable and for the maximum benefit of the group.
4. All departments must consider related party transactions with the Company or subsidiaries, or directors, or senior executives of the Company or subsidiaries having related interests that are not normal business operations or have different trading conditions from transactions with general customers or external parties by sending to the Company Secretary to review approval procedures for further action.
5. The Company discloses information on transactions that may have conflicts of interest or related party transactions and inter-company transactions according to criteria established by the Securities and Exchange Commission by disclosing in the annual registration statement and annual report or other report forms as applicable, and disclose related party transaction information to the Stock Exchange of Thailand according to Stock Exchange criteria, as well as transactions related to the Company according to accounting standard criteria.
6. The Company Secretary prepares forms to verify completeness of disclosure of inter-company transaction information in financial statement notes.
7. Internal auditors audit related party transactions according to audit plans and report to the Audit Committee with control measures, inspection, supervision to randomly review actual transactions correctly in accordance with contracts, policies, or stipulated conditions.

### 3. Important Issues for Consideration by Various Departments

1. Reasons and necessity for conducting transactions with related persons or parties or parties with conflicts of interest.
2. Reasonableness in terms of price and trading conditions when compared with transactions with other companies.
3. Operating procedures must comply with these requirements and regulations.
4. If independent appraiser or financial advisor opinions are required, bring them for consideration.

### 4. Criteria for Considering Normal Trading Transactions

- Transaction characteristics as normal business operations or not: If the transaction occurs due to normal operations, it will follow normal operating procedures in the same way as practiced with other items. Such inter-company transactions are in accordance with the Company's normal business and have reasonable grounds for conducting transactions to support normal business and to create maximum benefit to the Company with trading conditions not different from transactions with general customers or external parties.

- Fair prices and transaction conditions or not: If compared with transactions with unrelated external parties, would better prices or conditions be obtained?

  **Consideration of Prices According to Normal Trading Conditions (According to Stock Exchange Requirements)**

  Transactions in accordance with normal trading conditions are trading conditions having fair prices and terms that do not cause transfer of benefits by:

  - Prices and terms the Company or subsidiaries receive from or give to general persons
  - Prices and terms related parties give to general persons
  - Prices and terms the Company can demonstrate that business operators of similar nature give to general persons

## 5. Approval Procedures for Inter-Company Transactions or Related Party Transactions

The Company establishes transaction entry approvers using criteria for considering transaction size and conditions as specified in the Stock Exchange of Thailand Board Notification table regarding Information Disclosure and Operations of Listed Companies in Related Party Transactions with the following procedures:

1. Small Transactions: Transactions with value less than or equal to 1 million baht or less than or equal to 0.03 percent of net tangible assets, whichever is higher. Must be transactions with normal business or normal support conditions, whereby the Managing Director must not have interests in such transactions. Approved by Managing Director.
2. Small Transactions per Section 1: If the Managing Director has interests, approve by Executive Committee.
3. Medium Transactions: Transactions with value more than 1 million baht but less than 20 million baht or more than 0.03 percent but less than 3 percent of net tangible assets, whichever is higher. Approved by Executive Committee.
4. Large Transactions: Transactions with value more than or equal to 20 million baht or more than 3 percent of net tangible assets, whichever is higher. Considered by Executive Committee and proposed to Audit Committee for opinion to:
   - 4.1 Propose to Board of Directors for approval consideration
   - 4.2 In cases requiring shareholder approval, Board of Directors considers and gives opinion, and sends matter to Company Secretary to prepare documents and arrange shareholder meeting.
5. Quarterly: Executive Committee summarizes approved transactions in Sections 1, 2, and 3 to present to Audit Committee meeting for opinion consideration to report to Board of Directors.

### 9) Information Technology Security Policy

The Company is an organization that has adopted information technology to support and enhance operational efficiency. When information systems are unable to provide services or experience errors in service delivery for any reason, this may result in the Company's information technology systems and computer networks being unable to operate continuously and securely, which could negatively impact the Company's reputation or credibility. All users must cooperate in preventing damage or reducing the likelihood of damage to information technology systems and computer networks. Therefore, the Company deems it appropriate to establish an information technology security policy.

To ensure that all employees comply with the Company's and its subsidiaries' information technology security policy guidelines as outlined in the attached document (hereinafter referred to as "the Company") appropriately, efficiently, securely, and able to operate continuously, as well as to prevent problems that may arise from improper use of information technology systems and threats from various hazards, with the following objectives:

1. To establish an information technology security policy to ensure secure use of information technology systems, enabling efficient operations.
2. To define the scope of the information technology security management system.
3. This policy must be disseminated to all levels of employees in the Company and its subsidiaries for acknowledgment and strict compliance.
4. To establish standards, guidelines, and practices for executives, employees, and system administrators to recognize the importance of information technology security in operations and comply strictly.
5. To prevent any person from using any method to unlawfully access, modify, or destroy another person's data in the information system.
6. This policy must be reviewed and evaluated at least once per year.

The Company is committed to continuous development and improvement of work systems by adopting information technology and artificial intelligence (AI) systems to enhance operational efficiency, reduce errors, and support various processes within the Company in terms of data analysis and business decision-making. At the same time, the Company recognizes the importance of using such technology appropriately, responsibly, and being able to use such technology safely in creative work, as well as preventing risks that may arise from inappropriate use. Therefore, the Company has established an information technology security policy as follows:

1. To ensure that all employees work and use information technology and artificial intelligence (AI) systems correctly, appropriately, and efficiently, including being able to operate continuously, all employees must strictly comply with this policy.
2. To define the scope, standards, guidelines, and practices for managing information technology security, including artificial intelligence (AI) systems, with responsibility by considering ethical principles and data security, including protection of personal data of customers, employees, and the Company's data as a priority,

which must comply with applicable laws, rules, regulations, announcements, by-laws, or others, as well as prevent risks arising from misuse that cause impacts on individuals, offices, society, and the nation.

3. To establish review and revision of such policies at least once per year, or when there are changes in various risk factors that significantly affect the Company's business.

Definitions and Terms

**"Security"** means security for the Company's information technology system at Principal Capital Public Company Limited and its subsidiaries.

**"Measures"** means methods established as rules, regulations, procedures, or laws, etc.

**"Practices"** means details that specify step-by-step procedures that must be implemented to achieve standards set according to objectives.

**"Guidelines"** means approaches that are not mandatory to follow but are recommended to make achieving goals easier.

**"Executives"** means persons with senior management authority at Principal Capital Public Company Limited and its subsidiaries.

**"System Administrator"** means employees assigned by supervisors to be responsible for maintaining systems and computer networks, who can access computer network programs to manage computer network databases.

**"Employees"** means doctors, nurses, employees, permanent workers, and temporary workers.

**"External Persons"** means individuals or juristic persons other than doctors, nurses, employees, permanent workers, and temporary workers of Principal Capital Public Company Limited and its subsidiaries.

**"Information"** means facts obtained from data that have been processed and organized, which may be in the form of numbers, text, or images, into a system that users can easily understand and can be used for management, planning, decision-making, and other purposes.

**"Computer System"** means devices or sets of computer equipment connected to work together, with instructions, sets of instructions, or anything else and work practices defined for the devices or sets of devices to automatically process data.

**"Network System"** means a system that can be used for communication or transmission of data and information between various information technology systems of the Company as follows:

- **LAN System** means an electronic network system that connects various computer systems within the Company together as a network intended for communication and exchange of data and information within the Company.
- **WAN System** means a computer network system used for connecting over long distances, used to connect the head office with branch companies.

- **Internet System** means an electronic network system that connects various computer network systems of the Company to the worldwide internet network.

**"Information Technology System"** means an organization's work system that uses information technology, computer systems, and network systems to help create information that the organization can use for planning, management, service support, development, and communication control, which has components such as computer equipment, network systems, programs, work systems, and information.

**"Information Technology System Access Control"** means verification of approval and authorization to pass into information technology systems for users.

**"Server"** means a computer or operating system or computer program that provides one or more services to client computers or computer programs on the network system.

**"UPS Equipment"** means backup power supply and automatic voltage regulation equipment in case of problems with electricity supply, such as voltage drop, voltage surge, power outage, or power fluctuation, etc., whereby UPS equipment will continuously deliver quality power in all situations, as well as being equipment that helps prevent damage that can occur to electrical equipment and electronic equipment (especially computers and connected equipment), including functioning to supply backup power from batteries to electrical equipment or computers when electrical problems occur.

**"Generator"** means equipment that functions as a backup electricity generator.

**"Software"** means sets of instructions or programs used to command computers to work. Software therefore means sequences of work processes written with computer commands. These commands are arranged as computer programs. From what we already know, computers work according to commands. Basic work is merely operations on binary data, which represents data as numbers, letters, images, or even speech. Computer programs used to command computers are therefore software because they are sequences of computer work processes. One computer can work differently in many ways with different software. Software therefore includes all types of computer programs that enable computers to work.

**"Malware"** means malicious programs written to harm data in the system, such as causing computers to malfunction, stealing or destroying data, or opening channels for malicious actors to control computers.

**"Computer Virus"** means a type of program that has the ability to replicate itself into computer systems and, if given the opportunity, can spread to other computer systems, which may occur from using infected disks from one machine on another machine, or may spread through network systems or data communication systems as well.A computer being infected with a virus means the virus has embedded itself in the computer's memory. Since a virus is just a program, for a virus to be in memory, it must be called to run depending on the type of each virus. Usually users do not know they have activated the computer virus to run.

**"Sensitive System"** means a system that has high impact and importance to the organization.

**"Medical Record"** means a form for recording personal history, illness, and treatment data both in document form and electronic data for each patient who comes to receive examination and treatment services at any company in the Principal Healthcare Group.

**"Personal Data"** means data about individuals in information technology systems that enables identification of that person, whether directly or indirectly.

**"Personal Data Controller"** means a person or juristic person who has the authority to make decisions regarding collection, use, or disclosure of personal data.

**"Personal Data Processor"** means a person or juristic person who operates regarding collection, use, or disclosure of personal data according to the orders or on behalf of the personal data controller, provided that such person or juristic person operating in such manner is not the personal data controller.

## 1. Information Access Control and Usage

### Objectives

1. To control access to data and data processing equipment considering usage and security.
2. To establish rules regarding access permission, authorization, and delegation.
3. To ensure users understand and can strictly follow established guidelines and recognize the importance of information system security.

### Guidelines

**1.1 Information Access Control and Data Classification**

1. System administrators shall permit users to access the information system they wish to use only with approval from the responsible person/data owner/system owner as necessary for use only.
2. External persons requiring rights to use the Company's information system must request permission in writing from executives or authorized persons in the requester's chain of command.
3. System administrators must appropriately set data and data system access rights suitable for user access and user responsibilities in using the information system, and must regularly review access rights as follows:

3.1. Establish criteria for permitting access to use relevant information regarding permission, authorization, or delegation as follows:

3.1.1. Define rights for each relevant user group, such as:

- Read only
- Create data
- Enter data
- Edit
- Approve

- No rights

3.1.2. Establish criteria for suspending rights and delegation in accordance with User Access Management as defined.

3.1.3. Users wishing to access the Company's information system must request permission in writing and receive approval from authorized persons in the requester's chain of command or assigned system administrators.

3.2. Classification of data and prioritization or hierarchy of confidentiality of data:

3.2.1. Classify types of data into:

- Management information data, such as policy data, strategic data and commitments, personnel data, budget, financial and accounting data, etc.
- Medical information data, such as patient data, medical data, etc.

3.2.2. Classify data importance levels into 3 levels:

- Most important level data
- Medium importance level data
- Low importance level data

3.2.3. Classify data confidentiality hierarchy:

- Top secret data means if disclosed in whole or in part would cause the most serious damage, such as personal data that can identify individuals that may be related to laws or promulgated Acts that, when disseminated, may affect the Company.
- Confidential data means if disclosed in whole or in part would cause serious damage, such as tender data and prices set in the system, salary data, financial data.
- Internal use data means data used only within the organization, such as the Company's general statistics, inventory data.
- General data means data that can be disclosed or disseminated generally, such as general Company data available from external websites.

3.2.4. Classify access hierarchy:

- Executive level
- General user level
- System administrator or assignee level

3.2.5. Electronic document formats can be classified as follows:

- Text Format files produced from ordinary software tools. When opening files, text characters can be seen and read, which has several sub-formats such as TEXT Format, Document Format, PDF Format (Portable Document Format).

- Image Format files produced from software tools, formats used include JPEG Format, PNG or GIF Format, Bitmapping Format, etc.
- Multimedia document formats, such as animation, sound, and video.

4. System administrators must arrange for installation of recording and tracking systems for the Company's information system usage and monitor security violations against the information system.
5. System administrators must arrange for detailed recording of information system access and modifications to various rights as evidence for verification.
6. System administrators must arrange for recording of entry and exit to/from information system locations as evidence for verification.

1.2 User Access Management

1. System administrators must establish new user registration as follows:
   1.1. Prepare user registration forms for information technology systems.
   1.2. System administrators must verify user accounts to prevent duplicate registration.
   1.3. System administrators must verify and provide access rights appropriate to responsibilities (according to item 3 under "Information Access Control and Data Classification").
   1.4. System administrators must arrange for distribution of documents or written materials to users showing users' rights and responsibilities in accessing information technology systems.
2. System administrators must define usage of important information technology systems, such as computer application programs, email, wireless LAN systems, internet systems, etc., providing rights only for job duties and obtaining written approval.
3. System administrators must regularly review user accounts and usage rights at least once per year to prevent unauthorized system access by following these guidelines:
   3.1. Prepare a list of those who still have system rights separated by units of each Company and subsidiaries.
   3.2. Send such lists to supervisors of units of each Company and subsidiaries to review names and verify correct access rights.
   3.3. Correct various rights data according to feedback received from companies.
   3.4. Procedures for canceling usage rights upon resignation must be completed within 3 days, or when changing positions within must be completed within 7 days.
4. Password Management
   4.1. Establish password changes and cancellations when users resign or leave positions or cancel usage.
   4.2. Define usernames or user codes that must not duplicate.

4.3. Deliver temporary passwords to users by secure methods, avoiding use of other persons or sending unprotected email for password delivery.

4.4. Set the number of times users are allowed to enter incorrect passwords not exceeding 10 times.

4.5. Define that users do not record or store passwords in computer systems in formats that do not prevent access.

5. System administrators must manage access to data according to confidentiality levels in controlling access to each confidentiality level both direct access and access through work systems, including methods of destroying data of each confidentiality level.

6. In cases where special rights are necessary, such as rights outside of job responsibilities, such users must receive approval from authorized persons in the requester's chain of command and data access rights policy, with defined usage period and suspension immediately upon expiration or leaving position, and special rights received must be defined regarding what level can be accessed, and user codes must differ from normal user codes.

**1.3 User Responsibilities**

1. Password usage - users must comply as follows:

1.1. Users are responsible for protecting and maintaining their username and password information. Each user must have their own username and must not share with others, including not disseminating, distributing, or making passwords known to others.

1.2. Define passwords consisting of not less than 8 characters, which must include numerical characters, alphabet characters, and special characters.

1.3. Do not set personal passwords from one's own first or last name, or family members' names.

1.4. Do not use personal passwords for sharing files with others via computer networks.

1.5. Do not use computer programs to help automatically remember personal passwords (Save password) for personal computers that users possess.

1.6. Do not write or record personal passwords in places easily observable by others.

1.7. 1.7 Set initial passwords for users that are difficult to guess, and password delivery to users must be secure.

1.8. Users must change passwords every 3 months.

2. Any actions arising from use of a user's account that laws define as offenses, whether such actions arise from the user or not, shall be considered personal responsibility for which the user must take responsibility for offenses that occur.

3. Users must verify identity every time before using Company assets or information systems, and if such identity verification has problems whether from password locks or any errors, users must notify system administrators immediately by following these guidelines:

3.1. All types of computers before accessing operating systems must verify identity every time.

3.2. Using other computer systems on the network must verify identity every time.

3.3. Internet usage must verify identity and must record data that can identify the user.

3.4. When users are not at computers, must lock screens every time and must verify identity before every use.

3.5. All computers must set screen saver time by setting time at least 120 minutes.

4. Users must be aware of and careful in using data, whether such data belongs to the Company and subsidiaries or is external person data.
5. Confidential data in the custody of the Company and subsidiaries shall not be disseminated, modified, copied, or destroyed without authorization from authorized persons.
6. Users have a role in maintaining and being responsible for Company data. If loss occurs through misuse or unauthorized dissemination, users must share responsibility for such damage.
7. Users must protect and maintain confidentiality, accuracy, and availability of data as well as documents, recording media, computer data, or various information at risk of access by unauthorized persons.
8. Users have legitimate rights to store, use, and protect personal data as deemed appropriate. The Company and subsidiaries will provide support and respect for personal rights and will not allow any person to violate personal data without permission from the user possessing such data, except in cases where the Company and subsidiaries need to verify data or believe such data relates to the Company, whereby the Company and subsidiaries may appoint persons to verify such data at any time without notifying users.
9. Prohibited from opening or running Peer-to-Peer programs (meaning a method of organizing computer networks that defines all computers on the network as the same or equal, meaning each machine has its own programs or stored files, this arrangement allows use of programs or data files from any computer instead of having to use only from a File Server) or programs with the same level of risk, such as BitTorrent, Emule, etc., unless permission is obtained from authorized information technology approvers.
10. Prohibited from opening or running any type of online program unrelated to job duties.
11. Prohibited from using Company assets prepared for disseminating data, messages, images, or anything contrary to morality, national security, laws, or impacting Company missions.
12. Prohibited from using Company assets for disruption causing damage or use in data theft or anything contrary to laws and morality or impacting Company missions.
13. Prohibited from using Company assets for personal benefit.

14. Absolutely prohibited from performing any actions to intercept data, whether text, images, sounds, or anything else in the Company's information system network by any methods whatsoever.
15. Prohibited from disrupting, destroying, or causing the Company's information system to stop.
16. Prohibited from using the Company's information system to control external computers or information systems without permission from authorized information technology approvers or assignees for managing control of external computers or information systems.
17. Prohibited from any actions that constitute surreptitiously using or learning another's personal password in any case for purposes of accessing data or using resources.
18. Prohibited from installing equipment or performing any actions to access the Company's information system without permission from authorized information technology approvers or assignees for management.
19. Interconnected Business Information Systems - authorized information technology approvers shall consider various issues regarding security and laws, including various vulnerabilities before deciding to interconnect information technology systems, such as the Company and subsidiaries, companies, or companies requesting connection:
    19.1. Establish policies and measures to control, prevent, and manage shared data use.
    19.2. Consider limiting or not permitting access to personal data.
    19.3. Consider which personnel have rights or are authorized to access.
    19.4. Consider user registration matters.
    19.5. Do not allow system connection sharing in cases where systems do not have appropriate minimum security measures.

1.4 Assets Management

1. Users must not enter the computer network operations room (Operation Center) - meaning locations used for installing server computers and/or network management equipment - which are restricted areas under any circumstances, except with system administrator permission.
2. Users must not remove equipment or parts from computer network operations rooms except with system administrator permission.
3. Users must not connect tools or any equipment to the network for personal business purposes.
4. Users must not copy or make copies of data in the system before receiving permission, and users must not use or delete others' data under any circumstances.
5. Users have the right to use assets and various information systems that the Company has prepared for use for Company work purposes only. Users are prohibited from using assets and various information systems for activities not defined by the Company or causing damage to the Company.

6. Users must destroy important data on data storage media, data files before disposing of such equipment, and use techniques to delete or overwrite data on important data in storage devices before allowing others to continue using such equipment to prevent access to such important data, and will consider methods of destroying data on each type of storage media as follows:

| Storage Media Type | Destruction Method |
|---|---|
| Paper | Use document shredding machine |
| Flash Drive or all types of External Storage | - Overwrite original data multiple rounds<br>- Use crushing or grinding methods to damage |
| CD/DVD discs | Use document shredding machine |
| Hard disk | - Overwrite original data multiple rounds<br>- Use crushing or grinding methods to damage |
| Cloud Computing | The Company must prepare clear Service Level Agreements covering issues regarding roles and responsibilities of the Company and service providers including storage and data destruction when canceling or terminating service contracts, and the Company must comprehensively consider risks related to canceling cloud computing services to establish strategies and prepare cancellation/destruction plans to prevent or reduce impacts that may arise from risks such as service system disruption risks, information security and data confidentiality risks, processing system accuracy risks, etc. |

7. Any damage arising from violations according to item 5 shall be considered personal offenses for which users must take responsibility for damage that occurs.

1.5 Network Access Control

1. Measures for controlling entry and exit to server computer control rooms:
    1.1. All external company contacts must exchange identity cards such as national ID cards or driver's licenses with security officers to receive visitor badges, then record information in the logbook as specified in the "Entry-Exit Area Record" document.
    1.2. Unrelated persons and external company contacts bringing computer equipment or work equipment to operate in network system control rooms must record equipment lists in permission application forms for entry-exit as specified in the "Entry-Exit Area Record" document clearly and accurately.
2. Users bringing computers or equipment to connect with the Company's computer network systems must receive permission from authorized information technology approvers or assignees for management and must strictly comply with this policy. Users must have evidence of network connection requests.
3. No one may move, install additionally, or perform any actions on central equipment, namely routers, switches, equipment connected to the main network system without system administrator permission.
4. System administrators must control network system access to efficiently manage network systems as follows:
    4.1. Limit usage rights to control users to use only authorized network systems.
    4.2. Limit access routes to shared network systems (Access list and VLAN).
    4.3. Limit use of network routes from computers to server computers so users cannot use other routes.
    4.4. All Company network systems connected to other external network systems must connect through intrusion prevention equipment and must have the ability to detect malware.
    4.5. Network systems must install Intrusion Prevention System/Intrusion Detection System to monitor abnormal usage of persons accessing the Company's network systems.
    4.6. Entry to the Company's internal network system via the internet must have login records showing identity with usernames and must have authentication with passwords to verify user accuracy every time before use.
    4.7. Must prevent external companies connecting from seeing internal IP addresses of the Company's internal network systems.
    4.8. Prepare network diagrams with details about internal and external network system boundaries and various equipment, with updates to keep current at all times.
    4.9. Network device identification:
        4.9.1. System administrators keep network connection request accounts, namely requester names, computer details requesting service, IP addresses, and installation locations.

4.9.2. System administrators must limit users who can access equipment.

4.9.3. For equipment with external network connections, must identify device numbers indicating whether they can connect to internal networks or cannot connect.

4.9.4. Network equipment must be able to verify source and destination IP addresses.

4.9.5. Service requesters must complete "Network Connection Request" forms.

4.9.6. Accessing network equipment must verify identity every time equipment is used.

5. System administrators must manage and control servers and be responsible for maintaining servers in defining, modifying, or changing various values of systems software.
6. Installation or improvement of work system software must obtain approval from authorized information technology approvers or assignees for system maintenance before proceeding.
7. Establish storage of source codes, program libraries, and documents for work system software in secure locations.
8. Computer traffic data (Log) storage to ensure computer traffic data is accurate and can identify individuals according to Computer Act B.E. 2560 guidelines.
9. Establish measures controlling use of network systems and servers by external users to maintain system security according to the following practice guidelines:
    9.1. External company persons requiring rights to access the Company's network systems and servers must apply in writing for permission from authorized information technology approvers or assignees.
    9.2. Have strict control of ports used for system entry.
    9.3. Any methods that can access data or data systems remotely must receive permission from Company authorized persons, authorized information technology approvers, or assignees.
    9.4. Remote system access - users must provide evidence indicating reasons or necessity for operating with the Company adequately.
    9.5. Remote access to internal network systems and information systems in the Company must have login records showing identity with usernames and must have authentication with passwords to verify user accuracy every time before use.
10. Establish network separation as follows:
    10.1. Internet - separate networks into sub-networks according to various buildings to control unauthorized network access.
    10.2. Intranet - separate internal and external networks for safety in using internal information systems.
11. Clearly establish network protection and various equipment connected to network systems and must review configuration of various parameters such as IP addresses at least once per year. Additionally, defining, modifying, or changing parameter values must notify relevant persons every time.

12. All network systems connected to other external network systems must connect through intrusion prevention equipment or packet filtering programs such as firewalls or other hardware, and must have the ability to detect malware.
13. Must install Intrusion Prevention/Detection Systems to monitor abnormal usage of persons accessing the Company's network systems, by monitoring network intrusion, abnormal usage, and network system modifications by persons without relevant authority.
14. IP addresses of internal network work systems necessarily must be protected from external company connections being able to see them, to prevent external persons from easily knowing information about network system structures.
15. Using various tools for network system inspection must receive system administrator approval and limit use only as necessary.

1.6 Operating System Access Control

1. System administrators must establish new Company personnel registration (according to item 1 under "User Access Management") for usage as necessary and procedures for canceling usage rights (according to item 1 under "User Access Management") such as resignation or changing positions within the Company, etc.
2. Establish access procedures:
    2.1. Users must set passwords for using computers under their responsibility.
    2.2. After system installation completion, must cancel user accounts or change passwords for all default usernames that came with system installation immediately.
    2.3. Users must set screen saver programs to lock screens when not in use, after which when users want to use they must enter passwords to access.
    2.4. Before accessing operating systems must login every time.
    2.5. Users must not allow others to use their usernames and passwords to access Company computers together.
    2.6. Users must logout immediately when finished using or away from screens for long periods.
    2.7. Prohibited from opening or running Peer-to-Peer programs or risky programs unless authorized.
    2.8. Software the Company uses is licensed - users can request use as necessary for duties and users are prohibited from installing or using any unlicensed software. If discovered, it is considered a personal offense for which users are solely responsible.
    2.9. Software the Company provides to users is essential - users are prohibited from installing, removing, changing, modifying, or copying for use elsewhere.
    2.10. Prohibited from using all types of Company resources for commercial purposes.

2.11. Prohibited from presenting illegal information that infringes copyrights, displaying inappropriate text or images, or contrary to morality through the Company's network systems.

2.12. Prohibited from Company users controlling external computers or information systems without authorization from authorized persons.

3. User Identification and Authentication - require users to show identity with usernames and must have authentication with passwords to verify user accuracy every time before use.

4. Use of System Utilities - must limit and control use of utility programs for important computer programs because using some utility programs can allow users to bypass system security measures. To prevent violations or bypassing established or existing security measures, proceed as follows:

   4.1. Utility program usage must receive system administrator approval and must have authentication for accessing utility programs to limit and control usage.

   4.2. Utility programs used must not infringe copyrights.

   4.3. Must store utility programs separately from work system software.

   4.4. Limit rights of those authorized to use utility programs.

   4.5. Must cancel or delete utility programs and software related to unnecessary work systems and must prevent users from accessing or using utility programs.

5. Session Time-out establishment:

   5.1. Establish that information systems have usage time-out and close usage after no activity for 15 minutes.

   5.2. Establish that information systems have faster usage time-out for high-risk information systems.

6. Limitation of Connection Time:

   6.1. Establish that information technology systems have connection time limits for usage so users can use as long as possible within defined time periods and can only use during work periods defined by the Company.

   6.2. Establish that highly important information technology systems, work systems used in risky locations (public places or areas outside the Company) have connection time period limits.

1.7 Operating System Access Control

1. System administrators must establish new user registration (according to item 1 under "User Access Management") for usage as necessary and procedures for canceling usage rights (according to item 1 under "User Access Management") such as resignation or changing positions within the Company, etc.

2. System administrators must define usage rights for important information technology systems such as application programs, email, wireless LAN systems, internet systems, etc., providing rights only for job

duties and must receive written approval from authorized information technology approvers, and must regularly review such rights.

3. System administrators must set time periods for information system connections used for operating various information systems. When users have not used information systems for more than 15 minutes, the system will terminate usage. Users must login before entering information systems again.
4. System administrators must manage usage rights and personnel passwords as follows:
    4.1. Establish password changes and cancellations when system users resign or leave positions or cancel usage.
    4.2. Establish that users not record or store passwords in computer systems in formats that do not prevent access.
    4.3. Define usernames or user codes that must not duplicate.
    4.4. In cases where special rights are necessary for users, such users must receive approval from Company authorized persons, with defined usage periods and suspension immediately upon expiration or leaving position, and special rights received must be defined regarding what level can be accessed, and user codes must differ from normal user codes.
5. System administrators must manage access to data according to confidentiality levels in controlling access to each confidentiality level data both direct access and access through work systems, including methods of destroying data of each confidentiality level, as follows:
    5.1. Must control access to each confidentiality level data both direct access and access through work systems.
    5.2. Must establish usernames and passwords for use in verifying true identity of data users at each data confidentiality level.
    5.3. Define usage period and suspend immediately upon expiration.
    5.4. Transmission of important data through public networks should be encrypted with international standards such as SSL, TLS, VPN, or XML Encryption, etc.
    5.5. Establish password changes according to defined periods for data importance levels.
6. Sensitive systems that have high impact and importance must comply as follows:
    6.1. Separate sensitive systems from other work systems.
    6.2. Have their own environmental control with proportionally separated operating rooms.
    6.3. Define rights only for those with system usage rights.
    6.4. Use of mobile computers and communication devices (Mobile Computing and Teleworking) must comply as follows:
        6.4.1. Verify readiness of computers and equipment to be used for work regarding being ready for use and verify standard programs are correct according to licenses.

6.4.2. Be careful not to let external persons copy data from computers used, except for publicly disseminated data.

6.4.3. When no longer necessary to use mobile computing and communication equipment, must promptly return to responsible officers.

6.4.4. Officers responsible for returns must verify ready-use condition of returned mobile computing and communication equipment.

6.4.5. If damage that occurs arises from gross negligence by users, users must take responsibility for damage that occurs.

1.8 Software Licensing and Intellectual Property and Preventing Malwares

1. The Company emphasizes intellectual property matters. Therefore, software the Company authorizes for use or that the Company has licenses for, users can request use according to duty necessity, and users are prohibited from installing or using any unlicensed software. If violations are discovered, it is considered a personal offense for which users are solely responsible.
2. Software the Company has prepared for users is essential for work - users are prohibited from removing, changing, modifying, or copying for use elsewhere, except with permission from Company authorized persons, authorized information technology approvers, or assignees having rights to licenses.
3. User computers must install antivirus programs as announced by the Company for use.
4. All data, files, software, or anything else received from other users must be virus and malware checked before use or storage every time.
5. Users must update patches for operating systems to keep new at all times to prevent potential damage.
6. Users must be vigilant about viruses and malware at all times and when abnormalities are found, users must report incidents to system administrators.
7. When users find computers infected with viruses, users must not connect computers to networks and must notify system administrators.
8. Prohibited from surreptitiously copying, changing, deleting any data, messages, documents, or anything that is Company assets or others' assets without permission from authorized persons according to job chain of command.
9. Prohibited from disseminating computer viruses, malware, or any dangerous programs that may cause damage to Company assets.
10. Rights to develop any programs or hardware can proceed but must not proceed as follows:

10.1. Develop any programs or hardware that will destroy system security mechanisms including actions that constitute surreptitiously using passwords, surreptitiously copying others' data, or cracking others' passwords.

10.2. Develop any programs or hardware that give users rights and priority in possessing system resources more than other users.

10.3. Develop any programs that will self-replicate or hide programs with other programs in similar fashion to worms or computer viruses.

10.4. Develop any programs or hardware that will destroy software license restriction systems.

10.5. Present illegal information that infringes copyrights, displaying inappropriate text or images, or contrary to morality and good customs of Thailand, in cases where users create web pages on computer networks.

10.6. Outsourced Software Development:

10.6.1. Arrange for control of software development projects by external contractors.

10.6.2. Consider specifying who will have intellectual property rights for source codes in software development by external contractors.

10.6.3. Consider reserving rights to verify quality and accuracy of software to be developed by external service providers by specifying in contracts made with such external service providers.

10.6.4. Have malware inspection of various software before installation.

10.6.5. After delivery of software development from external companies, the Company must proceed to change various passwords to be ready for use.

## 1.9 Teleworking

1. Must prepare equipment for remote work, data storage, and communication equipment for remote users.
2. All remote users must pass identity verification. For increased security, must have verification such as passwords or encryption methods, etc.
3. Not permitted to use personal equipment to access the Company's information technology systems remotely if such equipment is not under control according to the Company's security policy.
4. Must establish procedures for approving requests, canceling, defining, or improving system access rights and/or returning equipment used for remote work.

## 1.10 Wireless LAN Access Control

1. System administrators must control wireless access point signals to minimize leakage outside wireless LAN usage areas.
2. System administrators must change default SSID (Service Set Identifier) values from manufacturers immediately when using wireless access points and establish hiding SSIDs.
3. System administrators must appropriately and securely set Wireless Security values as equipment can define for encrypting data between Wireless LAN Clients and wireless access points and set values to not display wireless network names.
4. System administrators choose to use MAC Address (Media Access Control Address) control methods and/or usernames and passwords of users with rights to access wireless LAN systems, by only allowing equipment with defined MAC addresses and/or usernames and passwords to correctly access wireless LAN systems.
5. System administrators must install firewalls between wireless LAN systems and the Company's internal network systems.
6. System administrators should establish that wireless LAN users communicate with the Company's internal networks via VPN (Virtual Private Network) to help prevent intrusion in wireless LAN systems.
7. System administrators must register all equipment used to contact wireless LAN systems.
8. System administrators must use software or hardware to verify wireless LAN system security to monitor and record suspicious events occurring in wireless LAN systems. In cases where abnormal wireless LAN usage is discovered, system administrators must report to authorized persons in the chain of command immediately.
9. System administrators must control and prevent unauthorized external persons or companies from using wireless LAN systems to enter intranet systems and various internal databases.
10. Users wishing to access the Company's wireless LAN systems must verify identity.
11. System administrators must register and appropriately define user rights for accessing wireless LAN systems suitable for responsibilities before entering wireless LAN systems, and must regularly review access rights. This must receive system administrator permission as necessary for usage.

### 1.11 Firewall Control

1. The Company is responsible for managing installation and configuration of all firewalls.
2. Initial firewall configuration must be set to deny all.
3. All services and internet connection routes not permitted by policy must be blocked by firewalls.
4. Internet users must login before every use.
5. Configuration of permitted services and connections must record changes every time if firewall values are changed.

6. Access to firewall equipment must only be accessible by those assigned for management.
7. Computer traffic data entering and leaving firewall equipment must send values for storage at computer traffic data logging equipment and must store traffic data not less than 90 days.
8. Policy establishment for providing internet service to client computers will open basic connection ports for commonly permitted general programs. If necessary to use connection ports other than defined, must receive consent from Company authorized information technology approvers beforehand.
9. Service configuration values of server computers in each network section must configure values permitting only connection ports necessary for service provision.
10. Must regularly backup various configuration data of firewall equipment every week or every time before changing values.
11. Server computers providing various internal Company information work systems that are intranet-like must not allow connections to use internet except when necessary by permitting on a case-by-case basis.
12. The Company has the right to suspend or block use of client computers with behavior violating policies or arising from operations of programs risky to security until resolved.
13. Remote Login connections from outside to servers or internal network equipment must record operations according to server and network equipment operation permission application forms and must receive approval from authorized persons beforehand.
14. Violators of firewall security policies will have internet usage suspended immediately.

1.12 E-Mail Control

1. Do not record or store passwords in computer systems.
2. Change passwords every 3 months.
3. Do not use others' email addresses to read, receive, or send messages except with consent from account owners, and consider email owners responsible for use of their emails.
4. After using email systems, must logout every time.
5. Sending confidential data should not specify data importance in email headers unless using Company-defined email data encryption methods. Be careful in specifying email addresses of recipients correctly to prevent sending to wrong recipients.
6. Prohibited from sending spam mail.
7. Prohibited from sending chain letters.
8. Prohibited from sending emails that constitute violations of laws or others' rights.
9. Prohibited from intentionally sending emails with viruses to others.
10. Must specify sender names in every sent email.

11. Must regularly backup email data as necessary (although the Company backs up email data, it is only for certain periods, therefore very old emails necessary for use need to be backed up by oneself).
12. Users must verify email attachments before opening to inspect files using antivirus programs to prevent opening executable files such as .exe, .com, etc.
13. Users must not open or forward emails or messages received from unknown senders.
14. Users must not use impolite language or send/receive inappropriate emails, data that may damage the Company's reputation, cause division between companies through emails.
15. Users must check their email boxes daily, should organize files and emails to minimize, and should delete unwanted emails from the system to reduce email system space usage.
16. Note - users should move emails to be referenced later to their computers to prevent others from secretly reading emails. Therefore, should not store unused data or emails in email boxes.

1.13 Internet Control

1. System administrators must define connection routes for computer systems to access internet that must connect through security systems the Company has allocated only, such as Proxy, Firewall, IPS-IDS, etc. Users are prohibited from connecting computer systems through other channels.
2. Personal computers and portable computers before connecting to internet through web browsers must have antivirus programs installed and patch operating system vulnerabilities.
3. Sending and receiving computer data through internet must have virus scanning by antivirus programs before every data transmission.
4. Do not use the Company's internet systems to seek commercial benefits personally and access inappropriate websites, such as websites contrary to morality, websites with content that may impact or threaten national security, religion, monarchy, or websites harmful to society or violating others' rights, or data that may cause damage to the Company.
5. Prohibited from disclosing important confidential Company work data not yet officially announced through internet systems.
6. Be careful downloading programs from internet systems. Updating programs must not infringe copyrights.
7. Using electronic bulletin boards must not disclose important and confidential Company data.
8. Using electronic bulletin boards must not present opinions or use language inciting slander that will cause damage to the Company's reputation, destroying relationships with other companies' personnel.

9. Users do not input any computer data that is false and constitutes offenses regarding national security, offenses regarding terrorism, or obscene images, and do not disseminate or forward such computer data through internet.
10. After finishing internet use, must logout from the system to prevent access by others.
11. Users must strictly comply with laws regarding computer-related offenses.

1.14 Personal Computer Usage

1. General usage guidelines:
    1.1. Computers the Company permits for use are Company assets used for work only.
    1.2. Programs installed on the Company's computers must be programs the Company has legally purchased licenses for. Therefore, users are prohibited from copying various programs and installing on personal computers or modifying or giving to others for illegal use.
    1.3. Not permitted for users to install and modify/change programs on Company personal computers.
    1.4. Moving or sending personal computers for repair must be done only by Company officers.
    1.5. Before using various portable storage media, must verify for viruses with antivirus programs.
    1.6. Users are responsible for maintaining computer security.
    1.7. Turn off personal computers in one's possession when daily use is finished.
    1.8. Set screen saver on computers under one's responsibility to lock screens after not using more than 120 minutes to prevent others from using computers.
    1.9. Prohibited from bringing personally-owned personal computers to use with the Company's network systems except after verification by the Company's system administrators before use.
    1.10. Must install reliable antivirus programs and update to latest always.
    1.11. Prohibited from using programs and software that infringe copyrights.
    1.12. Must register machines beforehand to use network systems.
    1.13. Users must study and follow user manuals carefully for safe and efficient use.
    1.14. Do not modify or add computer components and maintain computers in original condition.
2. Password usage:
    2.1. Users must store passwords confidentially.
    2.2. Do not write or record passwords and post in front of computers.
    2.3. Should change passwords every 3 months.
3. Prevention from Malware:
    3.1. Users must check for viruses from various media such as Floppy Disk, Flash Drive, and other Data Storage before using with computers.

3.2. Users must verify files attached to emails or files downloaded from internet with antivirus programs before use.

3.3. Users must verify any computer data with malware included that results in computer data or computer systems or other instructions being damaged, destroyed, modified, changed, or not operating according to defined instructions.

**1.15 Portable Computer Usage**

1. General usage guidelines:
    1.1. Portable computers the Company permits for use are Company assets used for work only.
    1.2. Programs installed on the Company's portable computers must be programs the Company has legally purchased licenses for. Therefore, users are prohibited from copying various programs and installing on personal computers or modifying or giving to others for illegal use.
    1.3. Users must study and follow user manuals carefully for safe and efficient use.
    1.4. Do not modify/change various computer components and maintain computers in original condition.
    1.5. In cases requiring moving portable computers, should use portable computer bags to prevent dangers from impacts such as falling from work tables or slipping from hands, etc.
    1.6. Avoid using fingers or hard objects such as pen tips to touch LCD screens causing scratches or causing portable computer LCD screens to break and be damaged.
    1.7. Do not place objects on top of screens and keyboards.
    1.8. Cleaning screens must wipe very gently and must wipe in the same direction - prohibited from wiping in circular motions because it will cause scratches on screens.
    1.9. Using portable computers for excessively long periods in very hot air conditions must turn off computers to rest machines for a period before turning on for use again.
    1.10. Moving machines while machines are turned on for use, lift from base under keyboards - prohibited from moving machines by pulling screens up.
2. Physical security:
    2.1. Users are responsible for preventing loss, such as should lock machines when not in use, not leaving machines in public places or areas at risk of loss.
    2.2. Users do not store or use portable computers in locations with high heat, humidity, dust, and must prevent dropping and impacts.
3. Operating system access control:
    3.1. Users must set usernames and passwords for accessing portable computer operating systems.
    3.2. Users must set quality and secure passwords.

3.3. Users must set screen saver programs by setting time approximately 15 minutes to lock screens when not in use, after which when wanting to use must enter passwords.

3.4. Users must logout from systems immediately when finished using or away from screens for long periods.

4. Password usage for users:

4.1. Users must store passwords confidentially.

4.2. Do not write or record passwords and post in front of computers.

4.3. Should change passwords every 3 months.

1.16 Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS

1. IDS/IPS Policy is policy for installing intrusion detection systems and network security inspection to protect information system resources and data on internal Company networks to have security as practice guidelines regarding network intrusion inspection with related roles and responsibilities.
2. IDS/IPS Policy covers all hosts on Company networks and all data networks including all routes data may travel that are not on internet routes.
3. All systems accessible from internet or public must pass IDS/IPS system inspection.
4. All systems in DMZ (Demilitarized Zone) must receive service pattern inspection before installation and opening for service.
5. All hosts and networks transmitting data through IDS/IPS must record inspection results.
6. IDS/IPS systems must regularly have Update Patch/Signature inspections.
7. Must have event inspection, traffic data, usage behavior, activities, and record traffic volume data entering networks daily by system administrators.
8. IDS/IPS will operate under basic firewall control rules used for accessing information system networks normally.
9. Servers with Host-Based IDS installations must have daily data inspections.
10. All usage behavior, activities, or events at risk of intrusion, system attacks, suspicious behavior, or system entry attempts both successful and unsuccessful must be reported to Company authorized persons immediately when discovered.
11. Suspicious activity behavior or abnormal system operations discovered must be reported to authorized persons in chain of command within 1 hour of discovery.
12. IDS/IPS systems have response patterns to occurring events, namely reporting discovery results of various events, proceeding according to procedures to reduce damage, deleting discovered malicious software, preventing events that may occur again in future, and proceeding according to plans.

13. The Company has the right to terminate network connections of computers with behavior at risk of system intrusion without advance notice to users.
14. Those verified as attempting any actions that violate Company policies, attempting unauthorized system access, system attacks, or having behavior risky to information system operations will have network usage suspended immediately. If such actions constitute offenses consistent with computer-related offense laws or actions that result in damage to the Company's data and system resources, must be prosecuted according to legal procedures.

**1.17 System Installation and Configuration**

1. Operating System Update:
    1.1. Verify servers and system equipment.
    1.2. Install operating systems exactly matching usage requirements.
    1.3. Define system administrator names and passwords, and usernames.
    1.4. Set configuration values, install computer names/IP addresses.
    1.5. Update/set operating system security level values (for operating systems with Service Patch Updates).
    1.6. Install Antivirus programs/update Virus Definitions and set system inspection scanning and program update configuration.
2. User Account Management:
    2.1. Define system administrator names and passwords.
    2.2. Define usernames and passwords.
    2.3. Record user accounts and system access rights.
3. System Security & Anti-virus Update:
    3.1. Monitor and watch computer system operations and system access.
    3.2. System performance or verify from installed security systems.
    3.3. Update/set security system values appropriately for problems.
    3.4. Update Antivirus programs and Definitions to be modern regularly every week.
    3.5. Proceed to scan for computer viruses regularly.
4. Database Management Operation:
    4.1. Install database management systems according to Company work system requirements.
    4.2. Set system or database program configuration values to work correctly and efficiently with operating systems as that database system defines.
    4.3. Create and define database administrator names, other usernames, and usage rights.
    4.4. Update/set system values appropriately modern or prevent problem occurrence always.

5. Install various work system program databases, set program system configuration, and define users and rights to access or reach databases:
    5.1. Install work system programs according to requirements or development.
    5.2. Set configuration or programs or services to work with operating systems according to those programs or work systems correctly and efficiently.
    5.3. Install databases and connect work systems and test service provision according to what those work systems define.
    5.4. Notify users or work system owners to be able to begin use by notifying names, passwords, and system and database access rights as defined.
    5.5. Define data backup criteria, number of copies, restore testing.
    5.6. Record configuration installation values and user accounts at each system level every time there is creation or improvement.

**1.18 Computer Traffic Data (Log) Storage**

1. Store computer traffic data (Log) on storage media that can maintain completeness, accuracy, authenticity, identify persons accessing such media, and data used for storage must define confidentiality levels for access.
2. Prohibited from modifying stored computer traffic data (Log).
3. Establish system operation recording, user operation recording (Application Logs), and intrusion prevention system detail recording, such as entry-exit system recording, system entry attempt recording, etc., for inspection use purposes and must keep recordings at least 90 days from when usage ended, by complying with computer-related offense laws.
4. Must have methods to prevent modification and changes to various recordings and limit access to such recordings only to relevant persons.
5. Log data management system planning should have planning and assessment for scope of storage and implementation.

**1.19 Database Security and Data Backup**

**Objectives**

1. To ensure Company information systems can provide continuous service.
2. To serve as standard practice guidelines and system administrator responsibilities in strictly operating for the Company and recognizing security importance.
3. To ensure users understand and can strictly follow established guidelines and recognize information system security importance.

**Guidelines**

**Database Security**

1. Define data and database rights and importance:
    1.1. Prepare database accounts, classify system or operation resource groups by defining user groups and user group rights.
    1.2. Establish criteria for permitting access to use relevant information regarding permission, authorization, or delegation as follows:
        1.2.1. Define rights for each relevant user group:
        - Read only
        - Create data
        - Enter data
        - Edit
        - Approve
        - No rights

        1.2.2. Establish criteria for suspending rights and delegation in accordance with User Access Management as defined.
        1.2.3. Users wishing to access the Company's information systems must request permission in writing and receive approval from Company authorized persons or assigned system administrators.
    1.3. Procedures for data storage:
        1.3.1. Classify types of data into:
        - Management information data, such as policy data, strategic data and commitments, personnel data, budget, financial and accounting data, etc.
        - Medical information data, such as patient data, medical data, etc.

        1.3.2. Classify data importance levels into 3 levels:
        - Most important level data
        - Medium importance level data
        - Low importance level data

        1.3.3. Classify data confidentiality hierarchy according to 4-level data confidentiality maintenance classification:
        - Top secret data means if disclosed in whole or in part would cause the most serious damage, such as personal data that can identify individuals that may be related to laws or promulgated Acts that, when disseminated, may affect the Company.

- Confidential data means if disclosed in whole or in part would cause serious damage, such as salary data, financial data.
- Internal use data means data used only within the organization, such as the Company's general statistics, inventory data.
- General data means data that can be disclosed or disseminated generally, such as general Company data available from external websites, hierarchical level for system administrators or assignees.

1.3.4. Classify access hierarchy.

1.3.5. Define access times.

1.3.6. Define number of access channels.

2. All types of information data in databases must receive protection level classification, authorized access or operation, and other necessary details for security measures.
3. Database-owning companies, authorized persons in chain of command shall consider user qualifications and programs authorized to perform any actions with such data according to rights and arrange for log files recording entry-exit for databases as necessary for purposes of verifying correct database usage.
4. In cases of databases shared between companies or exchanged or requesting data use from the Company, prepare data usage agreements or for information exchange between companies as follows:
   4.1. Establish policies, procedures, and standards to prevent data exchange between companies.
   4.2. Define roles and responsibilities of those involved and procedures for shared data use or data exchange, such as transmission and reception methods, etc.
   4.3. Define responsibilities for data protection.
   4.4. Establish procedures for verifying who sends data and who receives data to prevent denial.
   4.5. Define responsibilities for cases where exchanged data is lost or other damage events occur to such data.
   4.6. Define data access rights.
   4.7. Define technical standards used for data access or software.
   4.8. Establish special measures for protecting important data, software, or others, such as encryption keys, etc.

**Data Backup**

1. Consider selecting important information systems and appropriately prepare backup systems to be ready for use, ranked by priority from most to least necessary.

2. Define duties and responsibilities of officers for data backup.
3. Prepare accounts of all Company important information systems and establish information systems for which to prepare backup systems and prepare emergency preparedness plans at least once per year.
4. Establish data backup for each information system and define data backup frequency. For systems with frequent changes, define increased data backup frequency, by having data backup methods as follows:
    4.1. Define types of data requiring backup storage and backup frequency.
    4.2. Define data backup formats appropriate for data to be backed up.
    4.3. Verify various configuration values of data backup systems.
    4.4. Store backed-up data off-site - the distance between backup data storage locations and the Company must be sufficiently far not to affect data stored off-site in cases of disasters occurring to the Company and subsidiaries.
    4.5. Regularly test backup data recordings to verify they remain normally accessible to data.
    4.6. Prepare procedures for restoring damaged data from backed-up data.
    4.7. Regularly verify and test efficiency and effectiveness of data restoration procedures at least once per year or as appropriate considering various risks that will occur.
    4.8. Must prepare emergency preparedness plans in cases unable to operate by electronic methods to enable continuous normal information usage by:
        4.8.1. Defining duties and responsibilities of all involved persons.
        4.8.2. Having risk assessment for such important systems and establishing measures to reduce such risks, such as long power outages, fires, floods, earthquakes, protests preventing system access, etc.
        4.8.3. Having defined procedures for information system restoration.
        4.8.4. Having defined procedures for data backup and testing restoration of backed-up data.
        4.8.5. Having defined channels for contacting external service providers, such as network service providers, hardware, software, etc., when urgent contact incidents occur.
        4.8.6. Creating awareness or providing knowledge to officers involved with procedures or what must be done when urgent events occur, etc.
        4.8.7. Having reviews to improve such emergency preparedness plans to be appropriately and consistently applicable according to mission usage at least once per year.
        4.8.8. Must define duties and responsibilities of personnel who care for and are responsible for information systems, backup systems, and preparing emergency preparedness plans in cases unable to operate by electronic methods.

4.8.9. Must test ready-use condition of information systems, backup systems, and emergency preparedness systems at least once per year or as appropriate considering various risks that will occur so systems have ready-use condition always.

4.8.10. Have reviews of information systems, backup systems, and emergency preparedness systems sufficient for the Company's acceptable risk condition at least once per year.

## 1.20 Personal Data Collection, Use, or Disclosure

**Objectives**

To establish guidelines for protecting privacy of service users or those having business transactions with the Company, which apply to users and include external persons and companies involved with using the Company's information technology systems, as well as documents with personal data, which apply to users and include external persons and companies involved with using the Company's information technology systems.

**Guidelines**

1. Personal data of service users or those having business transactions with the Company related to information technology systems, in collection, use, disclosure (collectively called "processing") must comply with organizational privacy policy and information technology security policy.
2. Personal data of service users or those having business transactions with the Company in using information technology systems, collection, use, disclosure (collectively called "processing") that can directly or indirectly identify individuals must comply with provisions of laws, rules, announcements, orders, or regulations of relevant supervisory authorities or that will be amended.

## 1.21 Physical Security of Locations and Environment

**Objectives**

To establish measures for controlling and preventing security maintenance in using or accessing information system usage areas, by considering importance of information technology system equipment and data, which apply to users and include external persons and companies involved with using the Company's information technology systems.

**Guidelines**

1. Buildings, locations, and information system usage areas mean locations of computer systems, network systems, or other information systems, data preparation areas, computer storage and

equipment, computer personnel work areas, as well as personal computers and accessories installed permanently at work desks.

2. Computer network system control rooms must have the following characteristics:
   2.1. Defined as absolutely restricted areas or specifically restricted areas.
   2.2. Must be areas not located in areas with large numbers of people passing in and out.
   2.3. Must not have signs or symbols indicating important systems are inside such locations.
   2.4. Must lock doors, windows, or rooms always when staff are not permanently present.
   2.5. If necessary to use fax machines or copy machines, install separately from such areas.
   2.6. Absolutely not permitted to photograph or record moving images in such areas.
   2.7. Arrange areas for product delivery by separating from areas with information resources established to prevent system access by unauthorized persons.
3. Security area establishment:
   3.1. Have classification and appropriate definition of various information technology system areas for surveillance, control, security maintenance purposes from unauthorized persons, as well as preventing other damage that may occur.
   3.2. Define and clearly separate information technology system usage areas and prepare maps showing usage area positions and announce for general knowledge. Such area definition may be divided into General Working Area, System Administrator Area, IT Equipment Area, Data Storage Area, and Wireless LAN Coverage Area, etc.
4. Building and location entry-exit control:
   4.1. Clearly define users with entry-exit rights and time periods with entry-exit rights in each "usage area".
   4.2. For external persons or visitors entering Company buildings, security officers must have them exchange identity cards such as national ID cards, driver's licenses, etc., then record card data in logbooks and receive entry-exit forms along with visitor badges.
   4.3. Have recording of entry-exit dates and times to important areas for visitors.
   4.4. Visitors must wear badges visibly throughout time inside the Company.
   4.5. Contracted companies must wear badges visibly throughout work periods.
   4.6. Store entry-exit recordings for important areas or zones such as Data Centers, etc., for use in later inspection when necessary.
   4.7. Care for visitors in important areas or zones until missions are finished and they leave to prevent property loss or prevent unauthorized physical access.
   4.8. Have mechanisms for permitting external persons to access important areas or zones and must have adequate reasons for accessing such zones.

4.9. Create awareness for external visitors to understand rules or various regulations that must be followed while in important areas or zones.

4.10. Have control of access to areas with important stored or processed data.

4.11. Not permitted for uninvolved persons to enter important areas or zones except with permission.

4.12. Have identity verification, such as fingerprint scanning, password use, etc., to control entry-exit in important areas or zones (Data Center).

4.13. Arrange for care and surveillance of external persons' operations while operating in important areas or zones.

4.14. Arrange for review or cancellation of important area or zone access rights at least once per year.

5. Supporting Utilities:

5.1. Have sufficient work support systems for the Company's information technology systems' needs by having the following systems:

- UPS (Uninterruptible Power Supply)
- Generator (Backup Generator)
- Ventilation system
- Air conditioning and humidity control system

5.2. Have inspection or testing of such support systems at least once per year to ensure systems work normally and reduce risks from system operation failures.

5.3. Install alert systems to notify in cases where work support systems inside machine rooms work abnormally or stop working.

6. Cabling Security:

6.1. Avoid routing the Company's network signal cables in ways that must pass through areas accessible to external persons.

6.2. Have conduits for various signal cables to prevent signal interception or cable cutting to cause damage.

6.3. Route communication signal cables and power cables separately to prevent mutual signal interference and disturbance.

6.4. Make name tags for signal cables and on equipment to prevent incorrect line connection.

6.5. Prepare comprehensive and accurate communication signal cable maps.

6.6. Rooms with various communication signal cables must be locked securely to prevent external person access.

6.7. Consider using fiber optic cables instead of conventional communication signal cables (such as Coaxial Cable) for important information systems.

6.8. Survey all communication signal cable systems to find installations of signal interception equipment by malicious actors.

7. Equipment Maintenance:
   7.1. Have equipment maintenance schedules according to manufacturer-recommended time periods.
   7.2. Follow manufacturer-recommended maintenance instructions.
   7.3. Store equipment maintenance activity recordings for every service provision for later inspection or assessment use.
   7.4. Store problem and equipment defect recordings found for use in evaluating and improving such equipment.
   7.5. Control and supervise external service provider operations when doing equipment maintenance inside the Company.
   7.6. Arrange for approval of access rights to equipment with important data by external contractors (who do equipment maintenance) to prevent unauthorized data access through equipment access right approval request systems to authorized information technology approvers or assignees.
8. Removing Company Assets from Company:
   8.1. Have permission requests before removing such equipment or assets for use outside the Company.
   8.2. Define responsible persons for moving or removing equipment outside the Company.
   8.3. Define time periods for removing equipment for use outside the Company.
   8.4. When equipment is returned, verify consistency with permitted time periods and verify equipment damage.
   8.5. Record data on removing Company equipment for use outside the Company as loss prevention evidence and record additional data when equipment is returned.
9. Security of Equipment Off-Premises:
   9.1. Establish security measures to prevent risks from removing Company equipment or assets for use, such as transportation, accidents with equipment.
   9.2. Do not leave Company equipment or assets alone in public places.
   9.3. Officers have responsibility to care for equipment or assets as if they are personal property.
10. Secure Disposal or Re-use of Equipment:
   10.1. Destroy important data in equipment before disposing of such equipment.

10.2. Have measures or techniques for deleting or overwriting data on important data in storage equipment before allowing others to continue using such equipment to prevent access to such important data.

## 1.22 Information Risk Inspection and Assessment

### Objectives

1. To have information system risk inspection and assessment or undesirable or unpredictable security situations.
2. To prevent and reduce risk levels that may occur to information systems.
3. To serve as practice guidelines if risks dangerous to information systems occur

### Guidelines

**Part 1: Risk Inspection and Assessment**

Inspect and assess information risks or undesirable or unpredictable security situations that may occur to information technology systems at least once per year so organizations know risk levels and information security levels, with risk inspection and assessment guidelines to consider as follows:

1. Prioritize risks.
2. Find methods for proceeding to reduce risks.
3. Study advantages and disadvantages of methods for proceeding to reduce risks.
4. Summarize result recommendations and correction guidelines to reduce verified risks.
5. Have risk inspection and assessment and prepare reports with recommendations.
6. Have information system inspection and assessment measures at least as follows:
    6.1. Establish that inspectors can access necessary inspection data in read-only mode.
    6.2. In cases where necessary to access data in other modes, create copies for such data for inspectors to use and must destroy or delete immediately upon inspection completion or must store with very good protection.
    6.3. Establish identification and allocation of resources necessary for use in security management system inspection.
    6.4. Establish surveillance of system access by inspectors and record log data showing such access, including dates and times of accessing important work systems.
    6.5. In cases of information system inspection and assessment tools, establish separate installation of inspection tools from actual service systems or development systems and have storage protection of such tools from unauthorized access.

**Part 2: Risks that May Threaten Information Technology Systems**

From monitoring and inspecting various risks, including security incidents in information technology systems, threats can be classified into 5 types as follows:

Type 1: Threats from Organization Employees or Personnel (Human Error)

Such as employees or organization personnel lacking knowledge and understanding of computer equipment and tools in both hardware and software, which may cause information technology systems to be damaged, unusable, disrupted or stopped working, and may result in inability to use information technology systems at full efficiency. Initial operational guidelines have been established to reduce risk problems that will occur to information technology systems as follows:

1. Train organization employees to have basic knowledge and understanding of hardware and software to minimize human error risks, enabling employees to have knowledge and understanding of using and managing information tools and equipment in both hardware and software more efficiently, reducing risks arising from human error.

Type 2: Threats from Software that Damages Computers or Computer Network Systems

Consisting of computer viruses, internet worms, Trojan horses, and hoax virus news. These software types may disrupt operations and cause damage to information technology systems to the extent of making computer network systems unusable. Practice guidelines have been established to prepare for software threat situations as follows:

1. Install firewalls at server computers to function in defining server access rights and preventing external intrusions.
2. Install anti-virus software to intercept viruses entering network systems and be able to verify what types of viruses enter and damage computer network systems.

Type 3: Threats from Fire or Electrical Systems

Classified as serious threats that cause damage to information technology systems. Practice guidelines have been established to prepare for situations as follows:

1. Install UPS (Uninterruptible Power Supply) equipment to control power supply to server systems in cases of power failures. Computer network systems will be able to provide service for periods that allow safe data storage and backup.
2. Install smoke detection equipment. In cases of power failure incidents or smoke occurring inside network system control rooms, such equipment will send alert signals to security units to know and promptly enter to suppress emergency situations, with regular equipment readiness inspections.

3. Install gas-type fire extinguishing equipment in computer system control rooms for use in emergency situations (fires), with regular equipment readiness inspections and usage testing.

Type 4: Threats from Floods

Flood damage risks are classified as serious threats that damage information technology systems. Practice guidelines have been established to prepare for situations as follows:

1. Monitor flood threats by constantly following weather forecasts from the Meteorological Department.
2. Proceed to cut electrical systems in control rooms by turning off air conditioning circuit breakers to prevent control equipment damage and prevent electrical hazards.
3. Officers help move servers and network equipment to high ground.
4. When water recedes, have electricians verify electrical systems in network control rooms can be used normally and prepare network system control room readiness for installing servers and network equipment.
5. Install servers and network equipment and test usage of each server to verify they can provide service normally. Verify network systems can connect and provide service to client computers.
6. When verified that servers and network systems can provide data service properly, notify relevant units to enter for normal service use.

Type 5: Threats from Earthquakes

1. Monitor earthquake warning information, risk area data, disaster situation data from relevant agencies, and weather forecast data from worldwide meteorological agencies, namely:
    - Meteorological Department: Weather forecast data, temperature data, warning news (www.tmd.go.th)
    - National Disaster Warning Center: Advance warnings (www.ndwc.thaigov.go.th)
    - Department of Mineral Resources: Risk area data from landslides/earthquakes (www.dmr.go.th)
    - Earthquake Observation Division: Earthquake occurrence data (www.earthquake.tmd.go.th)
    - Department of Disaster Prevention and Mitigation: Warning notifications, risk area data, measures and practice guidelines (www.disaster.go.th)
2. Preparing people, evacuation locations, and materials/equipment:
    - Coordinate preparation work with rescue units to prepare for prevention and mitigation of earthquake and building collapse threats and define operation methods for all steps.

- Coordinate preparation with relevant government departments in preparing personnel, materials, and various equipment as necessary and appropriate.
- Survey safe evacuation locations with facilities, food, and drinking water for organization personnel.
- Prepare vehicles for evacuating disaster victims and transporting various necessary items.
- Do not place heavy objects on shelves, behind cabinets, or high places.
- Tie or secure heavy furniture to floors or walls.
- Study plans/practice emergency evacuation plans with clearly defined assembly points proportionate to each floor or unit.

## 1.23 Information Security Incident Response Operations

### Objectives

To establish measures for preventing intrusion and attacks or information system security violation incidents to have security.

### Guidelines

1. Intrusion Prevention System
    1.1. Proceed to verify log files or intrusion prevention system reports. Items to verify are as follows:
        - How many attacks occurred and what types of attacks were most frequent
        - Whether attack patterns that occurred have predictable formats
        - What level of severity
        - IP addresses of attacking networks
2. Firewall System
    2.1. Proceed to verify intrusion prevention systems at least once per month.
    2.2. Proceed to verify log file recordings and firewall reports. Items to verify are as follows:
        - Packets that firewalls blocked
        - Characteristics of blocked packets
        - Packets from which network IP addresses were blocked in large numbers

2.3. In cases of discovering system attacks or information system security violation incidents, notify organization authorized persons to decide on proceeding to solve problems.

3. Internet Threat Prevention System

Internet threats or malware consist of viruses, internet worms, Trojans, including spyware.

3.1. Proceed to verify log files and reports of equipment related to internet threat prevention systems. Items to verify are as follows:

- What types of malware were found in large numbers
- Which networks sent malware and where was it sent to
- Whether malware was sent from the Company's internal networks to outside

3.2. Study methods to fix computers infected with malware, especially malware types verified as distributed in the Company network.

3.3. When verified that computers inside the network are infected with malware or sending malware out, must suspend connection of malware-infected machines to network systems and immediately fix such machines.

**1.24 Artificial Intelligence Control and Usage**

The Company will use Artificial Intelligence (AI) systems that are researched, designed, developed, provided as services, and used with consideration of AI ethics principles as follows:

- AI systems must be researched, designed, developed, provided as services, and implemented ethically in accordance with generally accepted laws and standards.
- The Company respects and protects privacy and personal data of AI system users. AI systems must be designed and developed in accordance with personal data protection laws and must have strict security measures for personal data consistent with personal data protection policies to guarantee personal data privacy.
- AI systems must prevent and avoid having results from AI systems be biased, which would cause unfair discrimination, and the Company will arrange for regular inspection systems to detect and reduce bias that may occur.
- The Company will arrange for clearly responsible persons regarding AI system decisions and operations. Assigned persons must function in supervising compliance with laws and ethics of AI systems.
- AI systems must be transparent, meaning able to explain AI system processes and decisions that occurred retrospectively for stakeholders to understand and predict, with clear documentation and explanations provided to stakeholders.

- The Company will establish that humans can enter to judge and intervene in AI system decision-making processes, by preparing practice guidelines on when and how humans can intervene in AI system work processes.
- The Company will arrange for regular AI system assessment in terms of efficiency, effectiveness, ethical impacts, and compliance, as well as risk assessment and impact analysis that may occur, including arranging for reliable measures and/or processes to verify and confirm to users which content portions arose from using AI systems and which portions did not arise from using AI systems.

### 10) Information Technology System Usage Policy and Procedures

The Company supports employees and relevant workers in using information technology systems consisting of data communication network circuits, computers with peripheral equipment, data files, and Company data efficiently and in accordance with the Computer Crime Act B.E. 2550, as well as other relevant laws, for the Company's business interests with adequate data security standards.

**Usage Regulations**

1. This policy and procedures cover Company employees, subsidiary company employees, and other persons authorized to use information technology system services connected to the Company, both inside and outside the Company.
2. The Company permits only Company employees, subsidiary company employees, and other authorized persons to use the Company's information technology system services. The Company will register user names in a central database, and service users must strictly comply with this policy and procedures.
3. Information technology system services have the following service scope:
   - 3.1. Data communication network circuits and related equipment
   - 3.2. Electronic mail or email
   - 3.3. Intranet
   - 3.4. Standard PC software
   - 3.5. Internet web and internet mail service
   - 3.6. Remote work computer usage through Remote Access System such as Web Mail
   - 3.7. Specific application software
   - 3.8. Connecting PCs to information technology systems (External Link)
4. Password Usage
   - 4.1. Use only one's own password to access computers and networks according to received rights only, for purposes of protecting data security.
   - 4.2. Maintain password confidentiality to prevent others from seeing or easily discovering, and change initial passwords immediately upon receiving from the system or system administrators.

4.3. Change passwords used for entering networks every 90 days.

4.4. Passwords must be at least 8 characters long and difficult to guess, consisting of letters, numbers, or symbols.

5. Computer Usage

5.1. Turn off computers when finished using.

5.2. Lock computer screens with passwords using screensaver with password protect, and log out from computer systems by logging off or locking when away from computer screens for more than 15 minutes.

5.3. Store portable computer equipment (notebooks or PDAs) carefully to prevent loss, such as storing in safe places immediately upon leaving work desks.

5.4. Do not use computers as tools for committing offenses against the Company or others, such as improperly accessing network data and information systems, disrupting or causing annoyance to network operations and computer systems, intercepting data, surreptitiously decoding passwords, falsifying computer data, disseminating inappropriate images, messages, or sounds, and do not use computers to do anything illegal or actions showing intent deviating from normal usage behavior.

5.5. Employees must be responsible for messages, images, sounds, or data files sent from their own computers and be responsible for any damage that occurs if illegal actions are taken.

5.6. The Company reserves the right to control use of Company computers to ensure information system data security and does not permit employees to modify various machine parameter values, such as computer name, system configuration, program configuration. If needing to change various machine parameter values, must receive authorization from authorized persons and send to system administrators for changes.

5.7. The Company reserves the right not to permit employees to install computer programs independently, unless such employees perform duties in work related to program installation or have received authorization from the Company.

6. Computer Software Usage

6.1. Use computer software according to Company-defined standards. This excludes use of computer software for operational work, research work, or specialized work that units have procured for their own use.

6.2. Do not infringe computer software copyrights. If lawsuits from injured parties occur, violating employees must take responsibility for all damage that occurs.

6.3. Do not produce, possess, or distribute inappropriate or illegal computer software.

6.4. The Company reserves the right to inspect data on computers employees use if there are reasons to suspect employees are taking actions that may adversely affect the Company.

7. Internet Usage

    7.1. Do not use internet to seek commercial benefits personally, do not disseminate inappropriate data, do not access inappropriate websites, such as gambling websites, websites contrary to morality, websites with content opposing the nation, religion, or monarchy, or websites harmful to society.

    7.2. Do not use internet to download illegal or work-unbeneficial data or programs, such as movies, music, games, etc.

    7.3. Be careful using internet to access web boards and must not reference the Company's name in public web boards.

    7.4. The Company reserves the right to close access to inappropriate websites or websites that impact the Company's network operations.

8. Receiving and Sending Electronic Mail (E-mail)

    8.1. Be careful using electronic mail by preventing damage to the Company or creating conflicts between the Company and other persons, or creating misunderstandings, or violating others' rights, or creating annoyance to others, or being illegal, or violating morality, and do not seek benefits or allow others to seek commercial benefits from using electronic mail on the network, such as sending chain emails, sending emails to advertise products for sale, or disseminating news hoping for commercial results, etc.

    8.2. Do not send messages, images, sounds, or data files distributed to all employees without business reasons except when having direct duties to operations, whereby messages sent out must relate to Company work.

    8.3. Use polite language correct according to network usage customs or use language that polite people generally use in messages sent to other persons.

9. Instant Messaging (IM) Usage

    9.1. Use IM without causing damage to the Company or infringing copyrights, or creating annoyance to others, or being illegal, or violating morality, and do not seek benefits or allow others to seek commercial benefits from using IM.

    9.2. Do not chat or send confidential business data through IM.

    9.3. Do not use email accounts and passwords that duplicate Company email accounts and passwords when registering to use IM.

10. Computer Virus Prevention

    10.1. Do not adjust or cancel operations of antivirus programs installed for use on computers.

    10.2. Employees bringing computers for use outside Company networks, when bringing back for use on networks, must perform virus inspection before connecting to networks.

    10.3. Do not download data from inappropriate websites.

    10.4. Use caution if needing to open electronic mail received from strangers.

10.5. The Company reserves the right to suspend virus-infected computers or computers suspected of possibly bringing viruses to the Company from connecting to networks.

11. Data Confidentiality Maintenance and Protection

11.1. Do not access others' data without permission from data owners.

11.2. Do not print or copy data that has confidential classification levels of others, unless receiving permission from data owners.

12. Bringing Personal Computer-Related Equipment for Use on Networks

12.1. Do not bring personal computer data receiving-transmitting equipment, such as modems or wireless data receiving-transmitting equipment (WIFI) to connect with computers or networks, unless receiving approval from information technology system administrators.

12.2. Employees must request permission from information technology administrators before allowing external persons to bring all types of personal computers to connect to networks, and connection to Company networks will only use temporary passwords.

13. Remote Work Computer Usage Through Remote Access System (RAS) or Virtual Private Network (VPN) System

13.1. Employees must request permission from information technology administrators to request licenses to use computers through RAS or VPN and must not give RAS or VPN accounts to other persons for use.

13.2. Employees must be responsible for computer usage or any transactions made through such RAS or VPN.

13.3. The Company reserves the right not to permit computers currently entering RAS or VPN systems to connect to networks if there are suspicious reasons that such computers are unsafe for networks.

14. Computer Usage for System Disruption

Employees are prohibited from taking any actions intending to disrupt the Company's computer systems or external organizations' systems, such as disrupting computer system operations until unable to provide service.

15. Violations

In cases where the Company discovers user actions violating ethics and good morality, the Company will consider implementing disciplinary measures according to personnel policy and procedures for holders and/or service users violating this policy and procedures, which may include cancellation of information technology system service usage rights.

### 11) Personal Data Protection Policy (Privacy Policy)

Principal Capital Public Company Limited and its subsidiaries as per attached document (hereinafter referred to as "PRINC" or "we") respect privacy rights and place utmost importance on protecting personal data of job applicants, employees, probationary employees, former employees, service users, business partners, business allies, and all related persons. To ensure that PRINC will protect and treat your personal data in accordance with personal data protection laws, the Company has prepared this privacy policy (hereinafter referred to as "Policy") to establish guidelines and practices for implementing personal data protection.

#### Scope of Application

This Policy applies to job applicants, employees, probationary employees, former employees, service users, business partners, business allies, and all related persons of the Company, as well as those with direct duties in supporting implementation and compliance with this Policy.

In addition to this Policy, PRINC may establish privacy policies for PRINC's products or services to specifically clarify to personal data owners regarding personal data being processed, purposes and lawful grounds for processing, personal data retention periods, including personal data rights that personal data owners should have in such products or services.

In cases of conflicts in material substance between privacy notices and this Policy, the privacy notice for such service shall prevail.

#### Data Sources

1. Direct data you have provided in various activities, such as application procedures, registration, job application, contract signing, documents, surveys, or use of products, services, or other service channels controlled by PRINC, or when personal data owners communicate with PRINC at offices or through other contact channels controlled by PRINC, and including collection from personal data owners accessing websites, products, or other services according to contracts or missions.
2. Data from related third parties, such as relatives.
3. Data from automated systems, such as images from CCTV cameras, data from applications, or data from medical equipment.
4. Data from sources other than personal data owners, whereby such data sources have authority, lawful grounds, or have received consent from personal data owners to disclose data to PRINC, such as public data, partner agencies, business partners, Group companies.
5. In cases where personal data owners refuse to provide data necessary for PRINC's services, this may result in PRINC being unable to provide such services to such personal data owners in whole or in part.

## Legal Basis for Personal Data Collection

PRINC considers establishing legal basis for collecting your personal data according to appropriateness and service provision context. Legal basis for personal data collection that PRINC uses includes:

| Legal Basis for Data Collection | Details |
|---|---|
| For legal compliance | To enable PRINC to comply with laws governing PRINC, such as:<br>Laws for disease diagnosis and medical treatment, such as:<br>- Medical Facilities Act B.E. 2541<br>- Medical Profession Act B.E. 2525<br>- Public Health Act B.E. 2535<br>- Emergency Medical Services Act B.E. 2551<br>- Social Security Act B.E. 2533<br>Computer traffic data collection:<br>- Computer Crime Act B.E. 2560<br>- Official Information Act B.E. 2540<br>Tax laws<br>Including other laws, related announcements, and proceeding according to court orders, etc. |
| Necessary for legitimate interests | For legitimate interests of PRINC and other persons, whereby such interests are as important as fundamental rights in personal data owners' personal data, such as for security maintenance of PRINC's buildings and locations, or personal data processing for PRINC's internal affairs, etc. |
| Necessary for prevention or suppression of dangers to life, body, or health of persons | To prevent or suppress dangers to life, body, or health of persons, such as epidemic disease surveillance according to government policies, etc. |
| For contract performance | To enable PRINC to perform duties according to contracts or proceed with actions necessary for entering contracts whereby you are a contract party with PRINC, such as employment, work contracts, memoranda of understanding or cooperation agreements, or contracts in other forms, etc. |
| For historical document preparation, research or important statistics | To enable PRINC to prepare or support preparation of historical documents, research or statistics as PRINC may be assigned, such as preparing directories of directors or committee members, preparing statistics for digital government service usage, monitoring digital government policy implementation, etc. |

| Legal Basis for Data Collection | Details |
|---|---|
| Your consent | For collection, use, or disclosure of personal data in cases where PRINC necessarily must receive consent from you, with notification of purposes for collecting, using, or disclosing personal data before requesting consent, such as collecting sensitive personal data with purposes not according to Section 24 or 26 exemptions of the Personal Data Protection Act B.E. 2562, or presenting and promoting products and services of contract parties or business partners to you, etc. |

In cases where PRINC necessarily must collect your personal data for contract performance, legal compliance, or necessity for entering contracts, if you refuse to provide personal data or object to processing according to activity purposes, this may result in PRINC being unable to proceed or provide services as you requested in whole or in part.

### Purposes

PRINC proceeds to collect your personal data for multiple purposes, which depend on types of products, services, or activities you use, as well as characteristics of your relationship with PRINC or considerations in each context importantly. Purposes specified as follows are merely frameworks for PRINC's personal data usage generally. Only purposes related to products or services you use or have relationships with will apply to your data.

### Personal Data Security Maintenance

PRINC arranges for appropriate technical measures and management to prevent and maintain security of personal data, with encryption for data transmission through internet networks and controlling personal data access to only relevant persons, both for data stored in document and electronic formats. Such persons must firmly adhere to and strictly comply with PRINC's personal data protection measures, as well as having duties to maintain confidentiality of personal data they know from performing according to authority and duties.

Additionally, when PRINC sends, transfers, or discloses personal data to third parties, whether for service provision according to missions, contracts, or agreements in other forms, PRINC arranges for personal data processing agreements in processes of disclosing or forwarding personal data to external agencies or persons, to confirm that personal data PRINC collects will always have security.

### Data Protection Officer

PRINC has appointed a Data Protection Officer to function in monitoring, supervising, and providing advice on collecting, using, or disclosing personal data, including coordinating and cooperating with the Personal Data Protection Committee Office and preparing processes for notification when personal data breaches occur.

1. Arrange for regular training on personal data protection for employees.

2. Arrange for Record of Processing to record various activities in personal data processing and update to be current at all times. Personal data processing responsible persons must enter personal data processing activity information into systems the Company provides.
3. Verify personal data processing within the Company to comply with legal requirements.

### Complaints to Supervisory Authorities

In cases where you find that PRINC has not complied with personal data protection laws, you have the right to complain to the Personal Data Protection Committee or supervisory authorities appointed by the Personal Data Protection Committee or according to law. Before such complaints, PRINC asks you to please contact PRINC so PRINC has opportunities to receive facts and clarify various issues, including managing to resolve your concerns first at the first opportunity.

### Cross-Border Data Transfer

In some cases, PRINC may necessarily need to send or transfer your personal data to foreign countries to proceed according to purposes in providing services to you, depending on PRINC services you use or are involved with by activity.

If necessary to send or transfer your personal data to destination countries, PRINC will proceed so personal data sent or transferred has adequate personal data protection measures according to international standards, or proceed according to conditions to enable sending or transferring such data according to law, namely:

1. Complying with laws defining that PRINC must send or transfer personal data to foreign countries.
2. Notifying you and receiving consent from you in cases where destination countries have inadequate personal data protection standards, according to country lists announced by the Personal Data Protection Committee.
3. Necessary to perform contracts whereby you are a contract party with PRINC or proceeding according to your request before entering such contract.
4. Acting according to PRINC's contract with other persons or juristic persons for your benefit.
5. To prevent or suppress dangers to life, body, or health of you or other persons when you cannot give consent at that time.
6. Necessary to carry out missions for important public interest.

### Services by Third Parties or Sub-service Providers

PRINC may assign or procure third parties (personal data processors) to process personal data instead of or on behalf of PRINC. Such third parties may offer services in various characteristics, such as hosting, outsourcing, or work in other forms of contract work.

For assigning third parties to process personal data as personal data processors, PRINC will arrange for agreements specifying rights and duties of PRINC as personal data controller and persons PRINC assigns as personal data

processors, including defining details of personal data types PRINC assigns for processing, including purposes, scope in personal data processing, and other related agreements. Personal data processors have duties to process personal data according to scope specified in agreements and according to PRINC's orders only, and cannot process for other purposes.

In cases where personal data processors have sub-service provider assignments (sub-processors) to process personal data instead of or on behalf of personal data processors, PRINC will supervise personal data processors to arrange for agreement documents between personal data processors and sub-processors in formats and standards not lower than agreements between PRINC and personal data processors.

### Data Retention Period

PRINC will retain your personal data for periods only as long as such data remains necessary according to collection purposes, according to details defined in policies, announcements, or according to relevant laws.

When periods expire and your personal data no longer has necessity according to such purposes, PRINC will delete, destroy your personal data, or make your personal data no longer able to identify persons, according to formats and standards for deleting and destroying personal data that the Committee or laws will announce and define or according to international standards. However, in cases of disputes, rights exercises, or lawsuits related to your personal data, PRINC reserves rights to retain such data until such disputes have final orders or judgments.

### External Website or Service Connections

PRINC services may have connections to third party websites or services. Such websites or services may announce personal data protection policies with substance different from this Policy. PRINC recommends you study personal data protection policies of such websites or services to know details before accessing. PRINC has no involvement and no authority controlling personal data protection measures of such websites or services and cannot be responsible for content, policies, damages, or actions arising from third party websites or services.

### Personal Data Protection Policy Changes and Amendments

PRINC will review this Policy to be current at least once per year, or when there are changes necessarily requiring improvement, correction, or changes to this Policy as deemed appropriate, so this Policy has appropriateness to changing situations, and will notify you through website channels, email, or other channels by specifying the latest amendment date appended at the end. However, PRINC recommends please regularly verify to acknowledge new policies before disclosing personal data.

Accessing PRINC products or services after new policy enforcement is considered acknowledgment according to agreements in the new policy.

### Personal Data Owner Rights

1. Rights to access and receive copies of your personal data, including requesting disclosure of sources of your personal data that PRINC collected without receiving consent from you, except cases where PRINC has rights to refuse your requests according to law or court orders, and cases where your access and copy requests will affect and may cause damage to other persons' rights and freedoms. Rights to request access and receive personal data copies.
2. Rights to request correction of your personal data that is incorrect or incomplete, to be current, accurate, complete, and not causing misunderstandings.
3. Rights to request deletion, destruction, or making personal data become data that cannot identify persons when such data no longer has necessity or when personal data owners withdraw consent.
4. Rights to request the organization suspend use of your personal data in any one of the following cases:
    4.1 During periods when PRINC performs verification according to your requests to correct your personal data to be correct, complete, and current.
    4.2 When your personal data was collected, used, or disclosed unlawfully.
    4.3 When your personal data no longer has necessity for retention according to purposes PRINC notified you for collection, but you wish PRINC to retain such data for supporting exercise of your legal rights.
    4.4 During periods when PRINC is proving lawful grounds for collecting your personal data, or verifying necessity in collecting, using, or disclosing your personal data for public interest, resulting from your exercise of rights to object to collecting, using, or disclosing your personal data.
5. Rights to withdraw consent in processing data service users previously provided.
6. Rights to object to collecting, using, or disclosing your personal data, except cases where PRINC has grounds for refusing your requests lawfully.
7. Rights to request PRINC transfer personal data to other personal data controllers.

### Contact Channels

In cases of questions or wanting to inquire for additional details regarding personal data protection, data collection, use, or disclosure, rights exercise, or having any complaints, you can contact PRINC through the following channels:

### Data Protection Officer

Contact location : Principal Capital Public Company Limited, 29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63 (Ekkamai), Sukhumvit Road, Klongtan Nuea Sub-district, Watthana District, Bangkok 10110

Telephone : 02-009-2015

Data Protection Officers of subsidiary companies separated by each company, by notifying the following information for supporting personal data owner rights exercise:

- First name, last name, national ID card number/passport number
- Questions regarding personal data or rights you wish to exercise according to law
- Telephone number, address, and email that can be contacted back

### 12) Privacy Policy

Principal Capital Public Company Limited and its subsidiaries as per attached document (hereinafter referred to as "PRINC" or "we") are committed to protecting privacy and place utmost importance on protecting personal data of service users. To ensure that PRINC will protect and treat your personal data in accordance with personal data protection laws, we have prepared this privacy policy (hereinafter referred to as "Policy") to inform you of details regarding personal data operations, whether collection, use, and disclosure (collectively called "processing"), as well as various rights of personal data owners and contact channels with us as follows:

#### Purposes for Personal Data Processing

PRINC will proceed to process your personal data for the following purposes:

1. To provide or deliver medical services.
2. To create and store your medical treatment history data.
3. To make appointments, send notifications, coordinate between you and doctors, or provide health advice.
4. To coordinate and forward data to network hospitals and other medical facilities in cases of patient referrals.
5. To proceed with any accounting and financial activities, such as account audits, debt notification and collection, use of various welfare benefits, taxes, and transaction evidence as required by law.
6. For the hospital's legitimate interests, such as recording complaint calls through the Call Center system, recording images through CCTV cameras.
7. To use in investigations and compliance with laws, regulations, rules, or the hospital's legal duties.
8. To use data in verifying patient identity.
9. To use in business evaluation and improvement, product and service quality development, including advertising and public relations management.
10. To respond to your requests, such as receiving complaints.
11. For other purposes that receive explicit consent from you.

#### Personal Data Collected

"Personal data" means data about persons that enables identification of such persons, whether directly or indirectly, but does not specifically include data of deceased persons. In collecting and retaining personal data, PRINC will use lawful methods and limit only to what is necessary according to the aforementioned purposes.

Personal data that PRINC proceeds to collect includes:

1. Personal information, such as first name-last name, gender, date of birth, age, marital status, nationality, signature, photograph.
2. Contact information, such as registered home address, current address, telephone number, email, LINE ID, including information on various social media.
3. Official document data, such as copies of national ID cards, household registration, passports, work permits, or non-Thai national ID cards.
4. Financial information, such as billing information, bank account numbers, bank account page copies, credit or debit card information.
5. Data collected by the hospital or automatically from various hospital equipment, such as HN numbers, IP addresses, cookies, service usage behavior, service usage history, voice, photographs, moving images, Social Media account names, Chat, or Geolocation.
6. Service access data, such as doctor appointment data, relatives' personal data, and other supplementary services.
7. Newsletter subscription and marketing activity participation data, such as registration to attend seminars.

PRINC will proceed to collect and process personal data when receiving consent from personal data owners beforehand, except in the following cases:

1. For contract performance - cases of collecting, using, or disclosing personal data for necessity in service provision or contract performance between data owners and the hospital.
2. To prevent or suppress dangers to life, body, or health.
3. For legal compliance.
4. For PRINC's legitimate interests - cases where there is necessity for legitimate interests in PRINC's operations, whereby PRINC will primarily consider personal data owners' rights, such as to prevent fraud, maintain network system security, protect freedom and data owners' interests, etc.
5. For research or statistics - cases of historical document or archive preparation for public interest or regarding research or statistics whereby appropriate protective measures have been arranged to protect data owners' rights and freedom.
6. For government mission performance - cases of necessity for mission performance for public interest or performance of government authority duties that PRINC has been assigned.

### Sensitive Personal Data

"Sensitive data" means personal data regarding race, ethnicity, political opinions, cult beliefs, religion or philosophy, sexual behavior, criminal history, health data, health examination data, disability, labor union data, genetic data, biometric data, such as facial simulation data, iris simulation data, or fingerprint simulation data.

PRINC may necessarily need to collect and process sensitive data. The hospital will request consent from employees every time in collecting, using, and/or disclosing, except:

1. To prevent or suppress dangers to life, body, or health of persons.
2. As lawful activity operations with appropriate protection by foundations, associations, or non-profit organizations with purposes regarding politics, religion, philosophy, or labor unions provided to members, former members, or those having regular contact with foundations, associations, or non-profit organizations according to such purposes without disclosing such personal data outside foundations, associations, or such non-profit organizations.
3. As data publicly disclosed with explicit consent of personal data owners.
4. As necessary for establishing legal claims, complying with or exercising legal claims, or raising defenses against legal claims.
5. As necessary in legal compliance to achieve purposes regarding:
    5.1. Preventive medicine or occupational medicine, employee work capability assessment, medical disease diagnosis, health or social service provision, medical treatment, health management, or social welfare service system provision.
    5.2. Public health interests, such as health protection from dangerous infectious diseases or epidemics.
    5.3. Labor protection, social security, national health security, medical treatment welfare for those entitled by law, vehicle accident victim protection, or social protection.
    5.4. Scientific, historical, or statistical research or other public interests to achieve such purposes only as necessary, with appropriate measures arranged.
    5.5. Important public interests with appropriate measures arranged.

### Data Sources

1. Direct data you have provided in various activities, such as receiving treatment, answering questionnaires, subscribing to newsletters, participating in marketing activities.
2. Data from related third parties, such as relatives.
3. Data from automated systems, such as images from CCTV cameras, data from applications, or data from medical equipment.
4. Data from sources other than personal data owners, whereby such data sources have authority, lawful grounds, or have received consent from personal data owners to disclose data to PRINC, such as public data, partner agencies, business partners, Group companies.

### Personal Data Disclosure and Transfer

PRINC will not disclose and forward your personal data to external agencies, except receiving explicit consent from you or according to the following cases:

1. PRINC may necessarily need to disclose or share data only as necessary to business partners, service providers, or external agencies to achieve purposes specified in this Policy. PRINC will prepare personal data processing agreements as required by law.
2. PRINC may necessarily need to disclose or share personal data to Group companies, whereby data processing will be under purposes specified in this privacy policy only.
3. PRINC may necessarily need to disclose or share data only as necessary to government officials or agencies with authority, or having lawful orders, to proceed as required by law, such as reporting data required by law or disclosing personal data according to court orders, etc.

### Cross-Border Data Transfer

PRINC may send or transfer personal data to foreign countries, ensuring that destination countries or destination agencies have adequate privacy protection standards and policies.

### Personal Data Protection

PRINC will use appropriate technical measures and management to prevent and maintain security of your personal data, with encryption for data transmission through internet networks and controlling access to your personal data to only relevant persons, both for data stored in document and electronic formats, to prevent data loss or unauthorized access, destruction, use, modification, correction, or disclosure of personal data.

### Data Retention Period

PRINC will collect your personal data throughout periods only as long as necessary for processing according to purposes in this Policy, except where there is necessity to retain personal data for other reasons, such as to comply with laws or verify in case of disputes. PRINC may necessarily need to retain data for periods exceeding what is specified.

When such periods expire, PRINC will delete and destroy your personal data when such personal data no longer has necessity for use.

### Privacy Policy Changes

PRINC may consider improving, correcting, or changing this Policy as deemed appropriate, by announcing on websites of each Group company as per attached document, specifying the latest amendment date appended at the end. However, PRINC recommends please regularly verify to acknowledge new policies before disclosing personal data.

### Personal Data Owner Rights

1. Rights to access and receive copies of your personal data, including requesting disclosure of sources of your personal data that the office collected without receiving consent from you, except cases where PRINC has rights to refuse your requests according to law or court orders, and cases where your access and copy requests will affect

and may cause damage to other persons' rights and freedom. Rights to request access and receive personal data copies.

2. Rights to request correction of your personal data that is incorrect or incomplete, to be current, accurate, complete, and not causing misunderstandings.
3. Rights to request deletion, destruction, or making personal data become data that cannot identify persons when such data no longer has necessity or when personal data owners withdraw consent.
4. Rights to request the organization suspend use of your personal data in any one of the following cases:
    4.1. During periods when PRINC performs verification according to your requests to correct your personal data to be correct, complete, and current.
    4.2. When your personal data was collected, used, or disclosed unlawfully.
    4.3. When your personal data no longer has necessity for retention according to purposes PRINC notified you for collection, but you wish the office to retain such data for supporting exercise of your legal rights.
    4.4. During periods when PRINC is proving lawful grounds for collecting your personal data, or verifying necessity in collecting, using, or disclosing your personal data for public interest, resulting from your exercise of rights to object to collecting, using, or disclosing your personal data.
5. Rights to withdraw consent in processing data service users previously provided.
6. Rights to object to collecting, using, or disclosing your personal data, except cases where PRINC has grounds for refusing your requests lawfully.
7. Rights to request PRINC transfer personal data to other personal data controllers.

### Contact Channels

In cases of questions or wanting to inquire for additional details regarding personal data protection, data collection, use, or disclosure, rights exercise, or having any complaints, you can contact PRINC through the following channels:

### Data Protection Officer

Contact location : Principal Capital Public Company Limited, 29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63 (Ekkamai), Sukhumvit Road, Klongtan Nuea Sub-district, Watthana District, Bangkok 10110

Telephone : 02-009-2015

Data Protection Officers of subsidiary companies separated by each company, by notifying the following information for supporting personal data owner rights exercise:

- First name, last name, national ID card number/passport number

- Questions regarding personal data or rights you wish to exercise according to law
- Telephone number, address, and email that can be contacted back

### 13) Sustainable Development Policy

Principal Capital Public Company Limited ("the Company") operates medical business, healthcare services, and private hospitals. The Company is committed to developing the organization to grow sustainably with responsibility toward society and the environment, to continuously benefit all stakeholder groups: shareholders, investors, business partners, employees, society, and the environment.

With the organization's aspiration and commitment to being part of building foundations for communities—that is, having good health foundations—which aligns with the United Nations Sustainable Development Goals (SDGs), Goal 3: ensuring healthy lives and promoting well-being for all at all ages (Good Health and Well Being), the Company's business operations therefore uphold sustainable development principles as the core of business operations, integrating cooperation and building mutual understanding with all relevant parties. The Board of Directors and Executive Committee have approved driving business by adhering to guidelines according to sustainable development policies following the "3 Pillars" approach (Harmonized Hearts, Harmonized Care, Harmonized Values) as follows:

#### Harmony of Heart (ผสานใจ)

1. Create business growth by expanding the scope of quality medical treatment services at appropriate price levels to secondary cities or areas where public health services are not yet adequate for local demand. (Aligns with UN SDG 3: Good Health and Well Being)
2. Respect and emphasize preventing human rights violations, firmly uphold equality, treat employees equally, provide fairness in compensation, welfare, workplace safety and health, opportunities for career advancement, promote training to increase knowledge and develop skills, build bonds between employees and the organization, and support education for employees' children, youth in communities, and underprivileged persons in society. (Aligns with UN SDG 4: Quality Education, SDG 5: Gender Equality, and SDG 8: Decent Work and Economic Growth)
3. Focus on the "Prince Pasan" project: harmonizing work to communities, harmonizing people to hometowns, to jointly be part of stimulating community economies through promoting local employment, using local entrepreneurs, and integrating local identity into various business contexts. Promote employee participation in creating benefits for quality of life and economic development for society both inside and outside the organization, both directly and indirectly, through business processes and organizational activities. (Aligns with UN SDG 8: Decent Work and Economic Growth and SDG 11: Sustainable Cities and Communities)

#### Harmony of Stewardship (ผสานรักษ์)

1. Emphasize environmental management by considering potential impacts while upholding safety principles,

including efficient resource utilization and energy conservation. (Aligns with UN SDG 6: Clean Water and Sanitation, SDG 7: Affordable and Clean Energy, SDG 12: Responsible Consumption and Production, and SDG 13: Climate Action)

2. Create value and quality by focusing on developing services and products that reduce impacts or cause harm to consumers and the environment, to enable better quality of life meeting consumer needs. (Aligns with UN SDG 12: Responsible Consumption and Production and SDG 13: Climate Action)

Harmony of Governance (ผสานธรรม)

1. Create business growth with transparency, have good corporate governance policies, have organizational ethics considering interests of stakeholders, society, and the environment, have fair management and care for stakeholders, promote free trade without causing conflicts of interest, oppose corruption in all forms. (Aligns with UN SDG 16: Peace, Justice and Strong Institutions)

2. Support and promote stakeholder creativity, while continuously considering partnership cooperation to jointly develop innovations that enhance value to communities, society, and the environment alongside sustainable business growth together. (Aligns with UN SDG 17: Partnerships for the Goals)

### 14) Human Rights, Labor Rights, and Children's Rights Policy

The Company recognizes the value and equal human dignity of all personnel and stakeholders, and acknowledges internationally recognized human rights laws. The Company is also aware of business responsibilities toward children in all contexts, whether as patients, consumers, family members of employees, or members of communities surrounding operational areas. Therefore, the Company is committed to respecting human rights, labor rights, and comprehensively protecting and promoting children's rights, while emphasizing that all parties involved in the Company's value chain recognize the importance of and comply with laws, regulations, requirements, and good corporate governance to avoid violations of human rights, labor rights, and children's rights, including implementing appropriate measures or mechanisms to prevent, receive complaints, and remedy any impacts that may occur.

The Company has therefore established this Human Rights, Labor Rights, and Children's Rights Policy based on international human rights, labor rights, and children's rights principles, including the Universal Declaration of Human Rights (UDHR), the International Labor Organization (ILO) Declaration on Fundamental Principles and Rights at Work, the UN Guiding Principles on Business and Human Rights (UNGP), and UNICEF's Children's Rights and Business Principles (CRBP). The Company shall adhere to the following practices:

1. The Company and its personnel shall treat all persons according to human rights principles with equality based on human dignity without discrimination, and without segregation based on place of origin, race, nationality, gender and gender identity, age, religion, educational institution, expression of thought, physical condition, status, family

background, or any other differences, particularly for vulnerable groups including women, children, persons with disabilities, the elderly, and marginalized groups such as refugees and migrant workers.

2. The Company shall support and respect the protection of human rights, labor rights, and children's rights, and shall conduct business activities that do not directly or indirectly result in human rights violations of parties involved throughout the value chain.
3. The Company shall communicate and raise awareness regarding human rights, labor rights, and children's rights among personnel and relevant parties throughout the business value chain through appropriate channels.
4. The Company shall regularly conduct risk assessments and impact assessments on human rights, labor rights, and children's rights, both within the Company and among the Company's business partners, and shall establish appropriate guidelines or measures to manage such risks, including implementing measures to protect against and remedy such risk impacts.
5. The Company shall provide accessible and whistleblower-friendly channels for receiving complaints and tips regarding violations of human rights, labor rights, and children's rights within the organization or arising from the Company's business operations, including establishing effective complaint management systems and confidential data protection to safeguard informants.
6. The Company shall disclose policies and operations, including complaints regarding human rights, labor rights, and children's rights (if any), through annual reports and other appropriate channels.
7. The Company shall support personnel in exercising their rights as lawful citizens in accordance with the Constitution and applicable laws.
8. The Company shall consider recruitment and employment, compensation and benefits that are equal and non-discriminatory, provide learning and development opportunities, as well as equal and fair career advancement opportunities appropriate to the scope of duties and responsibilities.
9. The Company shall promote gender equality and support women's rights at all organizational levels, focusing on equal opportunities in employment, promotion, access to development and training, as well as eliminating the gender pay gap, and establishing policies and practices that promote a safe working environment free from sexual harassment and all forms of violence.
10. Personnel have the freedom to assemble and express opinions beneficial to the Company, provided such actions do not violate the freedom of others and remain within applicable laws, regulations, codes of ethics, and good social etiquette.

11. The Company shall support the establishment of a Welfare Committee, and personnel have the right to participate throughout the process and may propose opinions on employment conditions, working environment, and various benefits for the Company's consideration, which will benefit personnel overall.
12. The Company shall allocate appropriate working environments and workspaces for personnel in accordance with good occupational health and safety principles, and shall promote a working atmosphere that enables personnel to maintain good physical and mental well-being, including eliminating excessive working hours.
13. The Company does not support illegal employment of foreign workers, forced labor, human trafficking, and does not support the use of child labor under 18 years of age, except for educational career guidance purposes where schools and/or parents are informed, and in compliance with applicable legal regulations and requirements, both in its own business activities and throughout the business value chain.
14. The Company shall support and encourage personnel to be aware of and respect the customs, traditions, culture, beliefs, and faith of each locality.
15. The Company shall deliver quality products and services that are safe for health, hygiene, life, and property to customers according to their rightful entitlements, and shall establish appropriate standards of care for pediatric patients according to age groups, while fully, accurately, and sufficiently disclosing information to customers without concealment, distortion, providing false information, or causing misunderstanding that creates negative attitudes, incites social division, or promotes inappropriate values or wrong values toward and about children.
16. Company personnel must comply with contracts or agreements with customers fairly. In cases where compliance is not possible, personnel must communicate with customers (in the case of child customers, communicate with parents/guardians) to jointly find solutions and prevent damages, while treating all customers equally and equitably without discrimination, respecting privacy, and strictly maintaining customer data confidentiality.
17. In cases where personnel or parties involved throughout the value chain commit violations of human rights, labor rights, or children's rights, the Company shall take action in accordance with Company regulations or legal provisions and laws, based on fundamental principles of human rights, labor rights, and children's rights.
18. The Company shall support volunteer activities and projects to promote the well-being of vulnerable groups including children, and education for children, through collaboration with local authorities, schools, and relevant partners.
19. The Company shall support local employment and procurement, refrain from violating human rights of community members in any form, and invest in communities in connection with the Company's operational strategies.

This policy applies to all directors, executives, physicians, and personnel, including temporary contract employees, subcontractor employees, and any other employees acting under contract with and on behalf of the Company, as well as all

relevant parties throughout the value chain. The policy shall be communicated to all parties to ensure awareness of its importance and strict compliance.

### Communication Guidelines

1. Personnel shall receive communication regarding the Human Rights Policy from orientation and shall receive regular refresher training to emphasize the importance of such matters, in the form of training sessions or e-learning as appropriate.

2. Parties involved throughout the value chain shall receive communication through meetings, circulars, or disclosure through other appropriate channels.

### Complaint Channels

1) The Company provides channels for reporting complaints or tips regarding violations of human rights, labor rights, and children's rights in accordance with the Whistle Blowing Policy:

   a) For external parties, contact the Company Secretary:

      Website : Contact us at www.principalcapital.co.th

      Telephone : 02-009-2015

      Email : Princ_secretarywhistle@princgroup.com

      Mail : Company Secretary
      Principal Capital Public Company Limited
      29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63,
      Khlong Tan Nuea, Watthana, Bangkok 10110

   b) For employees, contact the Internal Whistle Blowing Committee:

      Email : Princ_internalwhistle@princgroup.com

      Mail : Internal Whistle Blowing Committee
      29 Bangkok Business Center Building, 23rd Floor, Soi Sukhumvit 63,
      Khlong Tan Nuea, Watthana, Bangkok 10110

2) Internal personnel may also report complaints or tips regarding violations of human rights, labor rights, and children's rights through communication channels directly to the Hospital Director as an alternative channel.

### Implementation Guidelines and Remediation Measures

1. The Company shall regularly conduct comprehensive human rights impact assessments or human rights due diligence to study the level of impact of human rights violation risks for individuals throughout the Company's value chain, and shall implement measures to prevent and mitigate such impacts based on identified issues.

2. The Company shall regularly monitor and track progress through both qualitative and quantitative indicators, using the results to develop or identify appropriate measures to manage such issues.

3. When complaints regarding violations of human rights, labor rights, or children's rights are received, the Company shall respond to such complaints straightforwardly and promptly, and shall protect complainants or whistleblowers through appropriate processes.

4. When impacts from violations of human rights, labor rights, or children's rights occur, the Company shall seriously remediate impacts arising from the Company and/or from parties involved or acting on behalf of the Company, and shall prioritize remediation according to the severity of impacts, including cooperating with various justice processes that serve as relevant mechanisms for remedying affected parties.

### 15) Tax Policy

The Company and its subsidiaries are committed to continuously adhering to good corporate governance policies and principles, with the ideals of conducting business with integrity, social responsibility, and building trust with all stakeholder groups. The Tax Policy complies with all tax laws and other related laws in a transparent, fair, and correct manner consistent with standards that align with the Company's business strategies and objectives. The Company has established the following Tax Policy:

1. The Company shall adhere to and comply with the laws and tax regulations of Thailand, emphasizing correct and complete tax compliance by appointing tax officers to coordinate and liaise with government tax authorities to provide accurate tax information that reflects the actual facts of business operations.
2. The Company shall not use irregular tax structures or tax structures created for tax avoidance purposes or to create complexity for tax benefits.
3. The Company shall plan, study, and analyze tax impacts in various aspects prior to investing in Company projects.
4. The Company shall establish transfer pricing for purchase, sale, or service transactions with subsidiaries appropriately in accordance with arm's length prices under normal market conditions.
5. The Company shall respect the government's rights to establish tax structures, tax rates, and tax collection mechanisms, maintaining open communication and coordination with tax regulatory authorities to build professional and efficient working relationships, and to ensure practices that are legally compliant.

**Definitions**

**"The Company"** means Principal Capital Public Company Limited (PRINC) or PRINC Group Companies.

**"PRINC Group Companies"** means the parent company, subsidiaries, and associated companies of Principal Capital Public Company Limited.

**"Board of Directors"** means the Board of Directors of Principal Capital Public Company Limited.

**"Director"** means a director of Principal Capital Public Company Limited and/or PRINC Group Companies.

**" Executive"** means the Managing Director, Chief Executive Officer, or Director of Principal Capital Public Company Limited and/or PRINC Group Companies.

**" Employee"** means employees, contract employees, and seconded workers of Principal Capital Public Company Limited and/or PRINC Group Companies.

**" Stakeholders"** means shareholders, customers, business partners, competitors, creditors, employees, society, communities, the environment, government agencies, and related organizations.

**"Review"** means the examination or verification of operations, methods, conditions, events, or various reports.

**" Connected Transactions"** means connected transactions as defined by the Stock Exchange of Thailand, or transactions between the Company or its subsidiaries and directors, executives, or related persons as defined under the Securities and Exchange Act, or transactions with related companies.

**"Related Company"** means a partnership or juristic person under Section 258 (3) through (7) of the Securities and Exchange Act B.E. 2535 (1992).

**" Conflict of Interest"** means the conduct of any activity where personal interests or interests of related persons, whether by blood relation or otherwise, influence decision-making that may obstruct or hinder the best interests of Principal Capital Public Company Limited and/or PRINC Group Companies.

**" Other Benefits"** means anything of value, such as discount cards, receipt of services or entertainment, receipt of training, or any other similar items.

**"Blood Relatives"** means father, mother, spouse, children, spouse of children, etc.

**" Related Persons"** means ancestors, siblings sharing both parents or sharing only father or mother, uncles, aunts (paternal and maternal), spouse, adopted children, etc.

## Principal Capital Public Company Limited

## Acknowledgment and Compliance Form

1. I have received the Company's "Corporate Governance Policy."
2. I will study and adhere to the Company's corporate governance principles and ethics as guidelines for conducting operations with the highest standards.

Signature.....

(.....)

Employee Number.....

Date...../...../.....

If you require clarification and/or additional explanation regarding any content appearing in this policy document, please contact the Company Secretary at Tel. 02-009-2015

(Original: Submit to Company Secretary)

## Principal Capital Public Company Limited

## Acknowledgment and Compliance Form

1. I have received the Company's "Corporate Governance Policy."
2. I will study and adhere to the Company's corporate governance principles and ethics as guidelines for conducting operations with the highest standards.

Signature.....

(.....)

Employee Number.....

Date...../...../.....

If you require clarification and/or additional explanation regarding any content appearing in this policy document, please contact the Company Secretary at Tel. 02-009-2015

(Copy)

## Sources/References


1. The Five Principles of Corporate Governance (2006 Revised Edition): Corporate Governance Center, The Stock Exchange of Thailand
2. Corporate Governance Code for Listed Companies 2017: The Securities and Exchange Commission
3. Securities and Exchange Act (No. 4) B.E. 2551 (2008)
4. Best Practices for Directors of Listed Companies: The Stock Exchange of Thailand
5. Corporate Governance Report: The Stock Exchange of Thailand
6. Handbook for Directors of Listed Companies: The Securities and Exchange Commission
7. Corporate Governance Assessment Criteria: Thai Institute of Directors Association
8. The Roles, Duties and Responsibilities of the Director of Listed Companies: DCP Program: Thai Institute of Directors
9. OECD Principles of Corporate Governance: Organization for Economic Co-operation and Development
10. Anti-Corruption Forum
11. Company Regulations