SFMI
ESG Policy

Samsung Fire & Marine Insurance

CONTENTS

Policy on Independence of BOD

Policy on Diversity of BOD

Prohibition of Workplace Harassment including Sexual Harassment

Safety and Health Management Policy

Personal Information Protection Policy

Tax Policy

Human Rights Policy

Policy on Responsible Investment

ESG Insurance Underwriting Policy

CODE OF CONDUCT

Samsung Fire & Marine Insurance Partners Code of Conduct

Customer Rights Policy

SFMI established requirements for independence of board of directors (BOD) to ensure its independence in compliance of the 「Commercial Act」 and 「Act on Corporate Governance of Financial Companies」 and has verified the level of independence of incumbent directors or director candidates based on the requirements.

Policy on Independence of BOD

1. Requirements for Independence

① A director shall not fall into any of the following items in Paragraph ① of Article 5 (Qualifications for Executive Officers) of the Act on Corporate Governance of Financial Companies.

② An outsider director shall not fall into any of the following items in Paragraph ① of Article 6 (Qualifications for Outside Directors) of the Act on Corporate Governance of Financial Companies.

「Act on Corporate Governance of Financial Companies」

▷ Article 5 (Qualifications for Executive Officers)

① The following persons shall be disqualified from being executive officers of a financial company:

1. A minor, a person under adult guardianship, or a person under limited guardianship;
2. A person declared bankrupt but not yet reinstated;
3. A person in whose case five years have not passed yet since imprisonment without labor or heavier punishment to which he/she was sentenced was completely executed (or is deemed to have been completely executed) or was remitted;
4. A person who was sentenced to the suspension of imprisonment without labor or heavier punishment, and is still in the period of suspension;
5. A person in whose case five years have not passed yet since a fine or heavier punishment to which he/she was sentenced under this Act or any other finance-related statutes was completely executed (or is deemed to have been completely executed) or was remitted;
6. A person who serves and served as an executive officer or an employee of a financial company in which case five years have not yet passed since any of the following measures was taken against the company (limited to persons specified by Presidential Decree as directly liable for the cause of such measures or those reasonably responsible for such measures):

(a) Revocation of permission or authorization for, or registration, etc. of, business under a finance-related statute;

(b) A measure of timely correction under Article 10 (1) of the 「Act on the Structural Improvement of the Financial Industry」;
(c) An administrative disposition under Article 14 (2) of the 「Act on the Structural Improvement of the Financial Industry」;
7. A person in whose case the period specified by Presidential Decree not exceeding five years for each category of sanctions has not yet passed since a sanction (including a notice equivalent to the relevant measure, in cases of an executive officer or an employee who has already retired or resigned from office) was taken against him/her under any finance-related statute for his/her conduct as an executive officer or an employee;
8. A person specified by Presidential Decree, by whom public interest and sound management of the relevant financial company or credit order are likely to be undermined.
② If a person appointed as an executive officer of a financial company falls within any category of paragraph ① 1 through 8, the person shall forfeit his/her position: Provided, That a person who falls within the category specified in paragraph ① 7 shall not forfeit his/her position in cases specified by Presidential Decree.

▷Article 6 (Qualifications for Outside Directors)
① The following persons shall be disqualified from being an outside director of a financial company: Provided, That a person may be qualified as an outside director, if the person becomes a specially related person of the largest shareholder under subparagraph 1 when he/she becomes an outside director:

1. The largest shareholder or a specially related person of the largest shareholder (referring to an executive officer or an employee of a corporation, if the largest shareholder or the specially related person of the largest shareholder is a corporation);
2. A major shareholder of the spouse or a lineal ascendant or descendant of a major shareholder (referring to an executive officer or an employee of a corporation, if the major shareholder is a corporation);
3. A person who serves as a full-time executive officer or employee or a non-standing director of the relevant financial company or its subsidiary (referring to a subsidiary defined by subparagraph 3 of Article 2 of the Monopoly Regulation and Fair Trade Act; hereafter the same shall apply) or who served as a full-time executive officer or employee or a non-standing director during the preceding three years;
4. The spouse or a lineal ascendant or descendant of an executive officer of the relevant financial company;
5. A full-time executive officer or employee of the company for which an executive officer or

employee of the relevant financial company serves as a non-standing director;
6. A person who serves as a full-time executive officer or employee of a corporation that has an important business relationship defined by Presidential Decree or a competitive or cooperative business relationship with the relevant financial company or who served as a full-time executive officer or employee of such corporation during the preceding two years;
7. A person who has served as an outside director of the relevant financial company for at least six years or who has served as an outside director of the relevant financial company or its subsidiaries for at least nine years in total;
8. A person specified by Presidential Decree, on any other ground, as a person who has difficulties in performing his/her duties faithfully as an outside director of the financial company or who is likely to influence the management of the relevant financial company.
② If a person who has become an outside director of a financial company falls within any category of paragraph ①, the person shall forfeit his/her position.
③ An outside director of a financial company shall be a person specified by Presidential Decree, from among persons who have abundant expertise or practical experience in finance, economy, business administration, law, accounting, etc.

2. Items for Verification

① Whether a person has abundant expertise or practical expertise required of an outside director of a financial company in finance, economy, business, accounting, law, or other relevant areas
② Whether a person can execute given tasks in a fair manner as an outside director, free from particular interests but for the benefit of all shareholders and consumers
③ Whether a person has an ethical mindset and a sense of responsibility required of an outsider director to undertake work
④ Whether a person can spend sufficient time and effort to fully undertake work as an outside director of a financial company

SFMI shall appoint directors based on the criteria of independence, fairness, integrity, and sense of responsibility, and organize the board of directors (BOD) with directors from diverse backgrounds and of vast experiences to ensure that the BOD can make important decisions from a broader perspective by considering interests of various stakeholders including shareholders and customers.

Policy on Diversity of BOD

1. SFMI shall appoint outside directors who meet the following requirements

① The BOD shall include directors from diverse backgrounds with experience and expertise appropriate for business implementation in the financial company.

② The company shall define diversity in a broad sense, and nominate and appoint candidates with sufficient work experience and expertise from diverse backgrounds in finance, economy, accounting, law, etc.

③ The company shall pursue balanced composition of the BOD by considering gender, ethnicity, nation, birthplace, etc., when appointing outside directors.

2. Executive Nomination Committee shall be managed fairly in accordance with the following standards and outside directors shall be appointed in a transparent manner.

① Structure of the committee (adequacy of the number of committee members, outside directors constituting a majority of the membership, authority and sense of responsibility of the members)

② Appropriateness of items on the agenda (discussion on the agenda between members and management, timeliness of document provision)

③ Management of Committee (documentation and review of meeting minutes, compliance with committee regulations)

3. The company shall disclose information on corporate governance and appointment of outside director in the following reports.

① Business report

② Annual report on corporate governance

SFMI protects employees against discrimination and harassment, and applies zero-tolerance principle to all sorts of workplace harassment including sexual harassment to ensure a safe and sound work environment for employees. To this end, SFMI implements the policy on prohibition of workplace harassment including sexual harassment as follows.

Prohibition of Workplace Harassment including Sexual Harassment

1. Preventive and Corrective Action on Sexual Harassment

(1) Definition of sexual harassment

Sexual harassment in the workplace refers to any unwelcome sexual advances, verbal or physical conduct of sexual nature, or requests for sexual favors by business owners, supervisors, or employees using their status in the workplace, which might reasonably be expected or be perceived to cause offense or humiliation or which could be used as a basis for hiring decisions and employment conditions.

(2) Prevention of sexual harassment

① SFMI shall provide education to prevent sexual harassment in the workplace at least once a year.

② Business owners, supervisors, and employees shall mutually respect one another, and commit to preventing sexual harassment in the workplace.

(3) Corrective action in the event of sexual harassment

Resolution process in the event of a sexual harassment case

① A victim of sexual harassment shall immediately take action on the personal level through refusal, warning, caution, etc. to the perpetrator and seek help from a counselor or supervisor, etc.

② A victim or witness of sexual harassment shall immediately report the case through harassment case reporting system or directly to HR department.
③ SFMI shall liaise the victim of alleged sexual harassment with an investigator to provide support in a swift manner.
④ The investigator shall physically separate the victim from the perpetrator and promptly conduct an investigation.
⑤ If the claim was confirmed as sexual harassment by investigation, the company shall take appropriate action on the perpetrator through an HR committee meeting in line with corporate by laws.
⑥ In case of any disagreement on the action by the HR committee, the case shall be subject to review by the HR Committee.

(4) Disciplinary action on perpetrator of sexual harassment

① HR Department shall refer the details of the claim provided by the investigator to the HR Committee.
② Once the case is referred, the HR Committee shall immediately hold a meeting to make a decision on employee transfer or disciplinary action, provided that the composition of the committee, procedure or type of a disciplinary action shall be determined in separate clauses.

2. Preventive and Corrective Action on Workplace Harassment

(1) Definition of workplace harassment

Workplace harassment refers to any conduct that inflicts physical or emotional harm to another employee by using one's status or relationship in the workplace, which deteriorates working environment.

(2) Prohibited workplace harassment conduct

Workplace harassment prohibited in the company includes the following:

① Physical threat or violence
② Incivility including repeated profanity or verbal abuse
③ Defamation such as spreading malicious rumors or gossiping about private life, slandering, and trolling on the internet
④ Unreasonable and repeated order to run one's personal errands
⑤ Unreasonable dismissal of others as incompetent, mockery or insult on one's performance
⑥ Workplace bullying or unreasonably isolating an employee from others in work assignment
⑦ Unreasonably and repeatedly assigning sub-par tasks for an employee's experience, expertise, and competency

⑧ Allocating no work for a considerable time period without a just reason

⑨ Behavior which inflicts physical or emotional harm to another employee by using one's status or relationship in the workplace or which deteriorates the working environment

(3) Prevention of workplace harassment

① SFMI shall develop and implement policies to prevent workplace harassment.

② SFMI shall provide education to prevent workplace harassment at least once a year.

(4) Corrective action in the event of workplace harassment

Resolution process in the event of a workplace harassment case

① Anyone can report workplace harassment upon acquiring knowledge of such case.

② The company shall take investigation without delay upon acquiring knowledge of workplace harassment or receive a claim of such case as in the foregoing paragraph.

③ The company shall take appropriate measures, such as change of workplace, order on paid leave, if deemed necessary to protect the victim or alleged victim of workplace harassment during the investigation, provided that the company shall not take any action against the will of the victimized employee.

④ If the claim was confirmed as workplace harassment by investigation, the company shall take appropriate measure for the victimized employee at the employee's request such as change of work site, reassignment and transfer, order of paid leave, etc.

⑤ If the claim was confirmed as workplace harassment by investigation, the company shall take appropriate action on the perpetrator without delay including disciplinary action, change of workplace, etc., provided that the company shall listen to the opinion of the victimized employee before taking such action on the perpetrator.

⑥ The company shall not dismiss or mistreat employees victimized by workplace harassment or employees reporting harassment cases.

SFMI established the Safety and Health Management Policy to reinforce safety and health management and comply with relevant laws and International standards including the Industrial Safety and Health Act and the ILO. Based on this policy, SFMI will identify all kinds of safety and health risks and continue to improve the results of safety management system in order to create a safe and healthy working environment.

Safety and Health Management Policy

1. General Provisions

(1) Purpose

The purpose of this policy is to set out safety and health management rules at Samsung Fire & Marine Insurance (hereinafter the "Company") to stipulate basic requirements for health and safety, the roles and responsibilities of safety and health managers and the management of safety and health organizations to preempt various risks and prevent human and physical damage. SFMI establishes safety environment goals to prepare for various risks such as human disasters, physical accidents, and violations of laws, and realizes safety and health management in detail through implementation plans, integration, and priority selection, and discloses its achievements every year.

(2) Scope of Application

① This policy shall apply to all employees, facilities, and equipment of the Company.

② This policy shall also apply to anyone entering a worksite of the Company and employees and workers of partner companies.

(3) Safety-first Principle

① All activities of the Company shall be implemented on the principle of safety and health management, and each worksite and department shall immediately respond to the direction or request for submission of materials by Safety Management Center.

② Each worksite and department shall prioritize the implementation of safety and health management and provide support in allocation of budget, human resources, transportation, etc.

(4) Definition

Terms used in safety and health management are defined as in the following.

① Occupational Accident refers to a situation where an employee dies, gets injured, or develops a disease during the course of work.
② Safety Management refers to activities to minimize loss and improve productivity by maintaining safety and preventing accidents at work.
③ Health Management refers to reasonable and structured management activities to maintain and improve mental and physical health of employees and prevent them from developing occupational illnesses.
④ Inadvertent Accident refers to a situation that may hamper the progress of work or lower its efficiency in the event of an unintentional unsafe action or condition, directly or indirectly causing human or financial loss.
⑤ Serious Accident refers to a severe case of industrial accident prescribed in the Enforcement Decree of the Ministry of Employment and Labor such as an accident leading to death.
· An accident with death of one or more persons
· An accident with simultaneous injury of two or more persons, which requires care for at least three months
· An accident with simultaneous injury or occupational illness of 10 or more people

(5) Priority on Safety and Health Management

Employees shall take safety as a top priority in all activities and management, and prioritize safety and health management in terms of budget, human resources, and system for accident prevention.

(6) Selection of Qualified Subcontractor

① A business owner shall award a contract to a qualified subcontractor with capacity to prevent industrial accidents.
② A business owner may assess safety management capability of the subcontractor, appropriate level of cost payment and its duration and reflect the result of the assessment on the contract before awarding the contract.

(7) Industrial Accident Prevention in Awarding Contract

In case where employees of a relevant subcontractor undertake tasks at a worksite of a contractor, the contractor shall comply with each of the following items:
① Organization and management of a consultative body composed of contractors and subcontractors
② Regular safety check on work sites
③ Support for subcontractors including provision of venues and materials for safety and health

education for employees of subcontractors

④ Check on completion of safety and health education for employees of subcontractors

⑤ Provision of venues for installation of facilities such as hygiene facilities stipulated by the Enforcement of the Ministry of Employment and Labor or cooperation on the use of hygiene facilities established by a contractor

⑥ Verification on the time and details of tasks, safety measures and health policies of subcontractors in case a contractor and subcontractor conduct work at the same place

⑦ Adjustment of time and details of tasks by subcontractors in case where there exist risks prescribed in the presidential decree such as fire and explosion as a result of mixed tasks

2. Organization and Responsibility

(1) Workplace Safety and health Committee

① The Workplace Safety and Health Committee shall review and deliberate on the following safety and health items:

· Development of plans for industrial accident prevention
· Development and modification of safety management regulations
· Safety and Health Education for employees
· Review and improvement of work environment
· Management of employee health
· Other relevant issues

② The Workplace Safety and Health Committee shall be composed of 8 people including four representatives from Employer (the Company) and four representatives from Employees, and shall be convened regularly on a quarterly basis.

(2) Safety and Health Management Organization

① Chief Safety and Health Management Officer shall have overall responsibility and authority over safety and health management of the Company.

② Safety and health Management Organization shall be organized and managed by separate standards.

③ Head of each team (department) shall faithfully implement safety and health management as the general manager of the team (department), and shall take responsibility for basic safety and health management of team (department).

(3) Chief Safety and Health Management Officer

Chief Safety and Health Management Officer shall govern and supervise safety and health management at work with authority over the following items:

① Development of industrial accident prevention plans
② Documentation and modification of safety and health management regulations
③ Safety and Health Education for employees
④ Measurement, review and improvement of work environment
⑤ Issues on health management including medical examination for employees
⑥ Investigation into the cause of an industrial accident and development of measures to prevent recurrence
⑦ Recording and maintenance of industrial accident statistics
⑧ Review on qualification of safety equipment and protective gear with regard to safety and health management
⑨ Other important issues related to safety and health measures

(4) Safety and Health Maintenance Manager

① Manager of headquarters, division, or individual department shall serve as Safety and Health Maintenance Manager.
② Safety and Health Maintenance Manager shall perform the duty of the following items for all employees stationed in worksites under their management:
· Provision of Safety and Health Education and training, if necessary
· Implementation of emergency actions in the event of an accident and reporting of results thereof
· Other safety and health issues
· Arrangement of equipment and materials, immediate implementation of remedial measures in risky situation, and reporting thereof
· Check on prevention of dangerous materials with fire risks(Indoor smoking, use of portable gas burner, fired heater, T-shaped power outlet, etc.)

(5) Duty and Responsibility

A person appointed as Safety and Health Manager responsible for occupational safety and employee health shall comply with this policy, implement safety and health management work, and take responsibility for any occupational accident in good faith. In addition, the Manager shall set annual goals and specific targets for safety and health, and prioritize and develop plans to meet the goals and targets.

(6) Reporting System

① A person who performs the duty of safety and health management shall immediately report an accident, to prevent delay in important decision-making in the event of an accident.

② Reporting shall be escalated to Safety and Health Maintenance Manager, Safety and Health Management Officer, Chief Safety and Health Management Officer, and CEO, and shall be completed within sixty minutes.
③ Reporting and remedial actions on any damage to facilities shall be proceeded win consultation with relevant departments including General Affairs Department and Real Estate Department.

3. Safety and Health Education

(1) Classification of Safety and Health Education

Safety and Health Education may be conducted on a regular basis to raise safety and health awareness of employees.

① Safety and Health Education shall be classified into regular education and special education by trainees.
② Occupational education shall refer to education provided by the Minister of Employment and Labor for safety and health staff appointed by law.

(2) Documentation and Management of Education Records

A managing supervisor shall record and manage the results of safety and health education. In case where the education is provided by a commissioned institution, the supervisor shall receive certificates or documents from the institution as the proof of education and preserve the records.

① Time and venue of education
② Education manager
③ Education course and content
④ Trainees and number of participants
⑤ Other requirements to prove the result of education

4. Safety and Health Management

(1) Development of Plan

① The Workplace Safety and Health Committee may develop annual work plans on safety and health management, inspection, education and training
② Chief Safety and Health Management Officer may develop safety and health management work plans.
③ Implementation of work plans shall be implemented systemically, and the results shall be reported to the Workplace Safety and health Committee.

(2) Safety Management Activities

① Safety Management Activities shall refer to systemic and premeditated activities to protect health

and wealth of employees from various risks and accidents.

② Safety Management Plan shall include the following items:

· Safety management procedures and plans

· Safety management inspection plans

· Education and training for accident prevention

· Budget for safety management

(3) Safety Inspection

① Safety inspection shall be conducted all year round with a special focus on entire inspection in the first half of a year and improvement and remedial actions in the second half of the year. Inspection plans shall include the following items:

· Overall information of inspection including objective, target, and scope of inspection

· Compliance with relevant laws, regulations, rules, and operating standards.

· Size and expertise of safety management staff, and adequacy of working environment

· Detailed inspection checklist for an objective evaluation

② For issues identified in a safety inspection to require improvement, Safety Manager or Health Manager shall take immediate action and report it to the Workplace Safety and Health Committee.

③ Safety Manager or Health Manager may conduct safety inspection internally within work sites against seasonal risk factors.

④ The company shall identify harmful elements and risk factors originating from tasks, assess the risk level, and take additional measures to prevent harm or health impairment for employees

· Recording and managing the results of risk assessment

· Adhering to relevant guidelines for risk assessment method, procedure, timing, and other necessary items

(4) Education and training

Safety and health Management Staff shall participate in education or training at least once a year, which shall cover the following items:

① Safety and health management goals and targets, compliance with Safety and health management

② Safety and health management work system, roles and responsibilities of staff

③ Consigned education in cooperation with central administrative institute

④ Drills in association with government agencies such as civic defense drills

(5) Culture of Workplace Safety

Safety and Health Management Staff shall continue to call for the following items to raise safety

awareness and establish the culture of workplace safety.

① Spreading the corporate culture to prioritize safety

② Production and promotion of video materials for accident prevention

(6) Medical Examination

① The Company shall conduct regular medical examinations at medical institutions to protect health of employees, and employees requested to have medical examinations shall not reject the request.

② Medical examinations prescribed in Paragraph 1 shall be classified into the following:

· Pre-assignment medical examination for employees in new assignment to hazardous departments or transition to such departments

· Common medical examination at least once every two years for all employees

· Special medical examination for employees who are constantly exposed to chemical factors, dust, noise, heat or employees who work night shifts.

- Employees working overnight between 10:00 p.m. and 6:00 a.m. at least four times per month during six months
- Employees working overnight between 10:00 p.m. and 6:00 a.m. at least 60 hours per month during six months

· Temporary medical examination to check whether an employee was addicted by harmful substances or other hazardous factors, and whether the employee developed a disease as a result, or to identify the cause of such disease

· Ad-hoc medical examination for employees who exhibit symptoms attributed by harmful factors at work, such as occupational asthma, occupational contact dermatitis, and other health problems or for employees who have doctor's medical opinions

③ The Company shall support various activities to protect mental health of employees as in the following items:

· Provision of various psychological counseling programs including online and offline consulting for individual employees and their families through psychological counseling center

· Support for psychological counseling for employees working in provincial areas in association with external counseling institutions

· Implementation of occupational stress test through medical history questionnaire in common health examination

④ Cases involving mental stress and health impairment from long-term emotional labor shall be handled in accordance with the Protection Guide for Customer Service Employees.

(7) Workplace Environmental Measurement

① Workplace environmental measurement shall be conducted on worksites exposed to chemical factors, dust, noise, or heat. However, the Company may forgo workplace environmental measurement in any of the following worksites:

· Worksites where work is done temporarily or for a short span of time
· Worksites that do not exceed the permissible limit of harmful substance consumption
· Worksites that do not involve dust-causing work
· Other worksites exposed to significantly lower levels of harmful substances than exposure limits designated and published by the Minister of Employment and Labor

② If harmful substances are found in workplace environmental measurement to exceed permissible levels, such fact shall be notified to relevant teams, which shall take appropriate actions including installation or improvement of facilities, and notify the result to Safety Manager.

(8) Suspension of Work by Business Owner

① All employees, subcontractors' employees, or anyone entering a work site of the company may suspend work and evacuate immediately in case where there exist urgent risks regarding the work site or facilities in the work site.

② Anyone who suspended work and evacuated shall report the fact to a managing supervisor or safety and health manager without delay.

③ A managing supervisor, etc.
* shall order suspension of work and evacuate employees without delay under urgent risks of industrial accidents.
* A managing supervisor, etc. refers to managing supervisor, safety and health manager, business owner, etc.

④ A managing supervisor, etc.
* shall take necessary safety and health measures to eliminate risk factors on the case of suspension of work.

⑤ A managing supervisor shall request advice if necessary by submitting relevant photos to a safety and health manager.

⑥ A managing supervisor shall check on safety measures at the work site and resume work in case where there is no problem.

⑦ A managing supervisor shall manage the records of suspension of work and notify a safety and health manager on a regular basis.

(9) Suspension of Work by Employees

① All employees, subcontractors' employees, or anyone entering a work site of the company may suspend work and evacuate immediately in case where there exist urgent risks regarding the work site or facilities in the work site.

② Anyone who suspended work and evacuated shall report the fact to a managing supervisor or safety and health manager without delay.

③ In the case of general public, the person shall notify an employee of the company, who shall report the situation to a managing supervisor or safety and health manager.

④ A managing supervisor or safety and health manager shall conduct an on-site inspection on the case of any suspended work and eliminate risk factors.

⑤ A managing supervisor shall request advice if necessary by submitting relevant photos to a safety and health manager.

⑥ A managing supervisor shall check on safety measures at the work site and resume work in case where there is no problem.

⑦ A managing supervisor (business owner) shall not put at a disadvantage employees who suspended work and evacuated from the work site in case where there exist a reasonable ground for the employees convinced of urgent risks of industrial accidents.

⑧ A managing supervisor shall manage the records of suspension of work and notify a safety and health manager on a regular basis.

(10) Promotion/Guide and Management

① A business owner or Chief Safety and Health Management Officer may provide education and promotion/guide to raise awareness sufficiently and suspend work under any urgent risks of industrial accidents.

② A business owner or Chief Safety and Health Management Officer shall create an environment and conditions for employees to determine suspension of work to prevent such risks.

③ A managing supervisor shall notify the suspension of work to a Health and Safety Manager, who shall compile and manage the data on a regular basis.

(11) Development and Installation of Safety and Health Mark

① A business owner shall install and post safety and health marks including the following items for employees to notice.

· Ban or warning on harmful or dangerous facilities or sites

· Direction or guide on emergency measures

· Other items required by relevant laws to raise employee awareness

② A business owner shall develop safety and health marks in a size easily noticeable to employees.

(12) Contingency Plan

① A managing supervisor shall develop a contingency plan including the following:

- · Preventive and responsive measures to contingencies such as a serious accident or fire explosion Scenario and solution by contingency case
- · Promotional measures with employees, facility users, nearby residents and environment taken into account
- · Mock drills on evacuation and response

② Other items required to implement a contingency plan shall be managed by BCM Policy of the company.

(13) Safety and Health Inspection on Facilities

① A managing supervisor shall identify risk factors at a work site early on to prevent any accident within the work site and conduct regular safety and health inspection on facilities to ensure public safety.

② A managing supervisor shall collect opinions from employees when conducting an inspection and improve facilities by reviewing issues raised by employees

③ The head of the department managing company buildings shall develop and operate specific plans on the period and method of safety and health inspection.

(14) Mock Drill on Evacuation and Response

A managing supervisor shall conduct mock drills on evacuation and emergency response including regular education by contingency scenario, and assess the results of the drills to make correction or complementation if necessary.

5. Accident Investigation and Emergency Measures

(1) Procedures in the Event of Accident

In the event of an accident, the witness shall immediately report the accident to a Safety and Health Maintenance Manager and take necessary emergency measures

(2) Emergency Measure in the Event of Accident

① In case where an accident occurred to an employee, colleagues and related parties shall take necessary measures such as transporting the employee to a nearby designated hospital or general hospital depending on the extent of accident and injury.

② In case where a chain of accidents is feared, necessary measures shall be taken including suspension of work, and evacuation of employees from the work site.

(3) Investigation and Reporting of Accident

① Chief Safety and Health Management Officer shall investigate into the site of an accident immediately after occurrence of an accident, and preserve the site until the completion of such investigation, without any intentional modification or destruction.

② In the event of an accident, Safety and Health Maintenance Manager shall report the accident without delay to Safety and Health Management Officer and Chief Safety and Health Management Officer.

③ The Company shall report any of the following items to the head of Regional Employment and Labor Administration in the given jurisdiction upon gaining knowledge of such serious accidents. However, when an accident occurs for any inevitable reason such as force majeure, the Company shall report the following items to the head of Regional Employment and Labor Administration without delay after the discontinuation of the accident :

· Overview of an accident and extent of damage

· Response measures and forecast

· Other important matters

④ Compensation for damage shall be provided at the earliest possible time in accordance with relevant laws and regulations.

⑤ Chief Safety and Health Management Officer shall document an Industrial Accident Questionnaire to report to the head of Regional Employment and Labor Administration in the given jurisdiction in case of an accident where a victim got injured or developed disease, which requires care for at least four days. However, compensation shall not be provided when application for care allowance or survivor's benefits was filed to Korea Workers' Compensation & Welfare Service within a month after the accident.

(4) Analysis of Accident and Response Measures

Safety and Health Management Officer shall analyze the cause of an accident, develop response measures, report them to Chief Safety and Health Management Officer, and implement such measures.

(5) Reporting Delay and False Reporting

Anyone who deliberately postponed reporting of an accident causing problems to safety management or testified false information shall be subject to disciplinary actions in accordance with these Regulations.

6. Prizes and Disciplinary Actions

(1) Principles of Prizes and Disciplinary Actions

A department or an employee with excellent safety and health management records shall be nominated as winners of prizes by the Workplace Safety and health Committee, and a department or an employee in violation of Safety and health Management Regulations and relevant laws, causing a considerable disadvantage to the Company, shall be subject to disciplinary actions by the Disciplinary Committee.

(2) Standards for Prizes

A person who falls into any of the following items may receive a prize in accordance with the Human Resources Regulations, and the type and procedure of prizes shall be governed by the Workplace Safety and health Committee.

① A person whose safety management proposal has been adopted
② A person who received an award from outside the Company in recognition of excellent safety and health management
③ A person who made a significant contribution to safety and health management

(3) Standards for Disciplinary Actions

A person who falls into any of the following items may be subject to disciplinary actions in accordance with the Human Resources Regulations, and such disciplinary actions shall be governed by the Human Resources Regulations.

① A person who caused an accident in breach of safety and health regulations, rules, standards, etc.
② A person who violated or failed to comply with an order or direction in safety and health management without a just reason
③ A person who procrastinated follow-up measures after an accident by concealment, false report, or negligence
④ A person who was warned at least twice by Chief Safety and Health Management Officer
⑤ Any other person who caused an accident by intention or material negligence, resulting in loss to the Company

(4) Warning

Chief Safety and Health Management Officer shall issue a warning whenever safety and health management including compliance with Safety and health Management Regulations, rules, standards, etc. is neglected, leading to an accident or a considerable risk of an accident.

7. Supplementary Provisions

(1) Emergency Contact

A network of emergency contacts shall be set up and managed to take swift actions in case of emergency to prevent human and financial loss.

(2) Safety Management of Partner Companies

Safety and Health Maintenance Manager shall engage partner companies in actively implementing safety management activities.

(3) Approval on Safety Work

In case where a subcontractor proceeds with construction in the premises of the company, the construction management company in charge of the construction shall gain safety approval from the managing director of the work site.

(4) Delegation of Work

① Chief Safety and Health Management Officer may delegate his or her tasks to a managing supervisor for a more efficient implementation of safety and health management on subcontractors.

② Chief Safety and Health Management Officer shall provide an active support for a managing supervisor to deliver the work of Chief Safety and Health Management Officer

③ A managing supervisor tasked with work of Chief Safety and Health Management Officer shall report the results or work or solutions to Chief Safety and Health Management Officer, who may take necessary measures in that regard.

[Appendix]

Safety and Health Management Principles

SFMI ensures the safety of customers and employees and complies with law and principles for accident prevention, prioritizing safety and health as the most important value in business management.

1. SFMI places the highest value on safety and health in all business activities.
2. SFMI top management always expresses resolution on safety and health and leads by example in business management.
3. SFMI complies with laws and regulations related to safety and health management and spreads the corporate culture of safety.
4. SFMI strives to enhance employee's health management and improve their working environment
5. SFMI provides the best support for the safety of sales organizations and partner companies and creates a culture of safety through mutual cooperation.

SFMI places a high value on users' information protection and proactively established policies on information protection. The company also develops and complies with guidelines on personal information protection.

Personal Information Protection Policy

1. General Provisions

(1) Purpose

This policy aims to set forth the specifics of technological, managerial, and physical measures implemented by Samsung Fire & Marine Insurance Co., Ltd. to protect personal information of customers and employees against loss, theft, leakage, falsification, or corruption in accordance with the Personal Information Protection Act and the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.

(2) Scope of Application

① This policy applies to anyone who performs duty in a contractual relationship with the company including but not limited to employees (both contract-based and outsourced positions), customers, and prospective customers.

② This policy applies to personal information of customers and employees, which is collected, used, provided, or managed through both information and communication networks for the purpose of providing services and means other than information and communications network.

③ Other matters not explicitly stated herein shall be determined by relevant laws, regulations, and bylaws of the company.

(3) Definition of Terms

The terms used in this policy shall be defined as follows.

① "Personal information " refers to information that pertains to a living person, such as the name and resident registration number by which the individual in question can be identified when the information is used alone or with other relevant data.

② "Subject of information" refers to a person who can be identified by the managed information and therefore is the subject of the given piece of information.

③ "Personal information file" refers to an aggregate of personal information systematically

arranged or organized according to specific rules in order for the personal information to be readily retrievable.

④ "Management" refers to the act of collecting, creating, interworking, recording, saving, holding, processing, editing, searching, correcting, recovering, using, providing, disclosing, or destroying personal information and other acts similar thereto.

⑤ "Personal information protection officer" refers to a general manager in charge of personal information protection affairs.

⑥ "Personal information manager" refers to an employee, dispatched worker, or part- time worker who handles personal information under the direction and supervision of personal information protection officer.

⑦ "Personal information management system" refers to a systemically organized system such as database to enable management of personal information.

⑧ "Password" refers to a string of secret characters entered into a system to verify the identity of an individual who has a proper authority to access an office computer or corporate communications network.

⑨ "Biological (bio) information" refers to bodily or behavioral data of an individual by which a person can be identified, such as fingerprints, face, iris, vein, voice, handwriting, and information generated from the data.

⑩ "Access history" refers to electronic records of the work performed by personal information manager when accessing personal information management system, including the account of personal information manager, access time, access spot, subject of information, work performed, etc. "Access" herein means a state where the personal information manager is connected to a personal information management system which enables data transmission or reception.

⑪ "Information and Communications Network" refers to information and communications system to collect, process, save, search, transmit, or receive information by using telecommunication facilities, telecommunication technologies, or computer technologies pursuant to Article 2 Paragraph 2 of the Telecommunications Basic Act.

⑫ "Authentication information" refers to information used to verify the identity of an individual requested by personal information management system or information and communications network management system.

⑬ "P2P(Peer to Peer)" refers to a computer network system to share files directly between network participants through information and communications network without the need for central coordination by servers. "Sharing settings" refers to an arrangement to allow other persons to browse, modify, or copy files of computer owners.

⑭ "Mobile device" refers to portable computing devices for wireless communications such as

mobile phone, tablet PC, etc.

⑮ "Auxiliary storage memory" refers to a memory to store files, either connected with or separated from the personal information management system and personal computer, such as portable hard disk(HDD), USB memory, CD(Compact Disk), DVD(Digital Versatile Disk), etc.

⑯ "CCTV" refers to a closed circuit television camera, which is placed in a specific space to record and transmit videos on people or objects for monitoring and surveillance.

⑰ "Intranet" refers to a private network used by an organization, which blocks or controls external access by physical network separation or access control system.

⑱ "Control terminal" refers to a terminal that directly access personal information management system to manage for management, operation, development, or security purposes.

2. Development and implementation of internal management plan

(1) Development and approval of internal management plan

① Information Security Department shall develop and implement the internal management plan for personal information with approval from CISO.

② Information Security Department shall acquire approval from CISO to revise the internal management plan.

(2) Proclamation of Internal Management Plan

The personal information protection officer proclaims the personal information internal management plan to make it available to employees by posting the plan on the company intranet.

3. Duty and responsibility of personal information protection officer

(1) Designation of personal information protection officer

① The Company shall designate a personal information protection officer in charge of personal information security work to prevent loss, theft, leakage, falsification, or corruption of personal information of customers, employees, or other individual persons

② The Company shall designate personal information protection officer in accordance with the Personal Information Protection Act and the Enforcement Ordinance of the Act.

Classification	Personal Information Protection Manager	Personal Information Manager
Department	CISO	Information Protection Security Dept.
Person in charge	Vice President Seong-ok Cho	Pro JoongWoo Lee
Office	02-758-4483	02-758-7783 (fax: 0505-161-0185)
e-mail	seongok.cho@samsung.com	Jw0819.lee@samsung.com

(2) Duty and responsibility of personal information protection office

Personal information protection officer shall perform his/her duty under the following items.

① Development and implementation of personal (video) information plan

② Regular examination and improvement of personal (video) information processing status and practice

③ Grievance resolution and damage redress associated with personal (video) information processing

④ Establishment of internal control system to prevent leakage, misuse, and abuse of personal (video) information

⑤ Development and implementation of education plan on personal (video) information protection

⑥ Protection, management, and supervision of personal (video) information files

⑦ Development, modification, and implementation of personal information management method

⑧ Management of materials related to personal information protection

⑨ Disposal of personal information, of which the management purpose has been achieved or the holding period has expired

⑩ Taking immediate action upon gaining knowledge of any breach of personal information and reporting to CEO if deemed necessary

(3) Duty and responsibility of personal information manager

① Personal information manager refers to an individual who collects, saves, manages, uses, provides, handles, or disposes of personal information of customers within the company, and may include regular workers, temporary workers, or contract-based workers.

② Personal information manager shall fulfill the following roles and responsibilities to protect customers' personal information.

- Participation in personal information protection activities
- Observance and implementation of internal management plan
- Compliance with technological, administrative, and physical standards to safeguard personal Information
- Review on any illegal or illicit violation of personal information by an employee or a third party
- Implementation of other tasks required to protect personal information of customers

4. Technological, managerial, physical safety measure for personal information management

(1) Management of access authority

① The Company shall establish and operate a framework to control access to personal information management system.

② The Company shall review the need for system access by personal information managers and grant them a required minimum authority to access personal information management system to a varying extent in accordance with their responsibility.

③ The Company shall modify or remove personal information managers' authority to access personal information management system without delay upon their retirement or transfer at work.

④ The Company shall keep the records of access authority to personal information management system including modification, removal, etc. for five years.

⑤ The Company shall issue a separate user account by personal information manager, when issuing a user account for access to personal information management system, and the account shall not be shared with other personal information managers.

⑥ The Company shall establish and apply password setting rules for personal information managers or subjects of information to use a safe password.

⑦ The Company shall establish and apply password-setting rules for personal information managers as set forth below.

· Set a password with at least 8 digits including alphabets, numbers, or special characters.

· Recommend not to use a password that is easy to guess, including personal information such as the birthday or phone number, or a series of numbers, or a password similar to the user id.

· Change the password at least once every quarter by setting an expiration date.

⑧ The Company shall take necessary technical measures for only authorized personal information managers to access personal information system, such as limiting access to personal information management system after multiple failed attempts with a wrong password or incorrect account information,

(2) Access control

① The Company shall take measures including the functions in the following items to prevent illegal access through information and communications network or infringement of personal information.

· Control unauthorized access to personal information management system by limiting access to internet protocol (IP) address, etc.

· Detect and respond to attempts to leak personal information by analyzing internet protocol (IP)

address, etc. that has accessed personal information management system

② The Company shall apply a safe access method including virtual private network (VPN), leased line, etc. and a safe authorization method including public key certificate, etc. for personal

information managers to access personal information management system through information and communications network outside the Company.

③ The Company shall take measures to control access to personal information management system, office computer, mobile devices, control terminal, etc. in order to prevent disclosure or leakage of personal information to unauthorized parties through internet web site, P2P, sharing settings, public wireless network, etc.

④ The Company shall check any vulnerability in the web site at least once a year and take necessary measures to prevent unique identification information from leakage, falsification, or corruption.

⑤ The Company shall shut down personal information management system automatically to prevent illegal access to personal information management system or infringement of personal information in case where personal information is left unattended by a personal information manager for a certain time period.

(3) Encryption of personal information

① The Company shall encode personal information including resident registration number, passport number, driver's license number, alien registration number, password, credit card number, account number, biological data, etc. through safe encryption algorithms to receive or transmit such information through information and communications network, forward them by using auxiliary memories, or save them in office computers or mobile devices.

② The Company shall store passwords by using a one-way encryption to prevent them from decoding.

③ The Company shall encode unique identification information to store them in the internet zone and in the Demilitarized Zone (DMZ) between the internet and intranet firewalls.

④ The Company shall encode users' personal information and authentication information by installing a safe security server to receive or transmit such information through information and communications network, and the security server shall be equipped with any of the following functions in the items set forth below.

- A function to install a sockets layer (SSL) certificate in a web server to encode and transmit information
- A function to install an encryption application program in a web server to encode and transmit information
- A function to install a VPN in other internet to encode and transmit information

⑤ The Company shall establish and enforce procedures on creation, use, retention, distribution, and disposal of a safe encryption key to store encoded personal information in a safe manner.

(4) Retention and review of access history

① The Company shall take a regular examination and supervision on the access records of personal information management system by personal information managers on a monthly basis, and retain and manage the history for at least two years to check on any irregularities on the system.

② The Company shall store the access records by personal information managers through a regular back-up in a separate storage memory to prevent any falsification, theft, or loss of the access history.

③ The Company shall monitor cases of personal information downloaded through personal information management system and investigate the reason why it has been downloaded.

(5) Installation and management of security program

The Company shall install and operate a security program such as vaccine software to prevent or remove malware, etc. and observe in the following.

① Use automatic update of security programs or execute daily update to keep the security programs up to date

② Execute an immediate update in case where a malware warning has been issued or security update has been notified by production companies of application programs or operating system software.

③ Delete identified malware, etc. or other responsive measures

(6) Internet site security

In the case of web sites managing personal information (collection, use, access, search, etc.) among internet sites (including cyber work sites) under direct management by the company or in commissioned operation, the Company shall acquire a prior written consent by relevant departments in each phase from web site development to modification or removal of major functions, except the representative web site of the Company (www.samsungfire.com).

(7) Disposal of personal information

① The Company shall dispose of personal information without delay when the purpose of personal information management is achieved, when it has passed the retention period, or when the personal information is rendered unnecessary, except for cases where it needs to maintain the information in accordance with other laws and regulations.

② Other specific items on the disposal of personal information shall be determined by separate guidelines.

(8) Physical safety measure

① The Company shall develop and operate access control procedures in case where it operates a physical storage containing personal information such as computing room and data archive.

② The Company shall maintain documents and auxiliary memories containing personal information in a place with safety locks.

③ The Company shall develop safety measures to control the use of auxiliary memories containing personal information.

(9) Emergency preparation and safety measures

① The Company shall establish emergency response manuals to protect the personal information management system in case of emergency such as fire, flood, power failure, and natural disaster.

② Personal information managers shall develop plans to back up and restore personal information management system in case of emergency such as fire, flood, power failure, and natural disaster.

(10) Risk analysis and response

Risk analysis and responsive measures shall be determined in a separate guide.

(11) Protective measure in printing or copying

① The Company shall confine the purpose of printing personal information in the personal information management system (print, screen display, file generation, etc.) and minimize printing items in accordance with the purpose.

② The Company shall develop protective measures for printing and copying of personal information to manage paper documents or external memories containing such information in a safe manner.

(12) Installation and management of CCTV

① The Company shall inform its CCTV installation and operation to the subject of information by taking necessary measures including installation of signage containing information in the following items.

- Purpose and site of installation
- Scope and time of recording
- Name and contact information of managing staff
- Name of contact information of trustee in case where installation and operation of CCTV has been entrusted

② The Company shall not use or provide personal video data to any third party for any purpose other than the intended objectives, except for the cases in the following items:
- In case where the Company acquired approval from the subject of information
- In case where there are special regulations stipulated in other laws and regulations
- In case where it is clearly deemed necessary for urgent protection of life, body, or property of the subject of information or a third party, when the subject of information or his/her legal agent is not available to express intent, or where a prior consent cannot be obtained because of an unknown address, etc.
- In case where personal video data is provided for the purpose of statistics compiling or academic research with individuals in the video have been illegibly blurred

③ The Company shall delete personal video data without delay upon the expiration of the retention period prescribed in the CCTV operation and management guidelines, except for cases where there are other special regulations stipulated by law.

④ The Company shall record and manage the following items in case where it uses personal video data for any purpose other than its intended objectives or provides the data to any third party
- Title of personal video data file
- Name of user or recipient of personal video data (public institution or individual)
- Purpose of use or provision
- Legal ground for use or provision (if any)
- Period of use or provision (if any predefined time period)
- Type of use or provision
- The Company shall record and manage the following item to dispose of personal video data.
- Title of personal video information subject to disposal
- Date of disposal of personal video data (disposal cycle and disposal result in the case of automatic deletion on predesignated disposal dates)
- Staff in charge of disposal of personal video data

(13) Development and disclosure of personal information management rules

① The Company shall develop and disclose the specifics under the following items in accordance with Article 30 of the Personal information Protection Act.
- Objective of personal information management
- Period of personal information management and retention
- Provision of personal information to any third party
- Entrustment of personal information management
- Rights and duty of the subject of information and legal agent and their exercise

· Name of personal information protection officer, title and contact information of department in charge of personal information protection and grievance resolution thereof
· Installation and operation of devices collecting personal information such as internet access files, and denial thereof
· Other personal information management items stipulated by the Personal Information Protection Act

② The Company shall keep posting personal information management guidelines on its internet web site.

(14) Entrustment of personal information management

① The Company shall educate and supervise a trustee by reviewing the information management status, etc. to prevent loss, theft, leakage, falsification, or corruption of personal information of the subject of information, in case where it entrusts personal information management.

② Other specific items on the delegation of personal information management shall be determined by separate guidelines.

(15) Enterprise Risk Management

Risks on personal information shall be managed by enterprise-level SFMI operating risk management system.

5. Disciplinary Action on Violation of Information Security

(1) Procedures on Disciplinary Actions

In the event of violation of security regulations or internal bylaws, the security manager shall assess the level of disciplinary actions pursuant to Article 24 herein and notify the assessment to HR Team. The Information Security Committee shall review the level of assessment and refer the case to the HR Committee, which shall make the final decision on the disciplinary action.

(2) Standards on Disciplinary Actions

① The level of disciplinary actions to be applied to a violator shall depend on the graveness and intentionality of the violation, and a senior employee in charge of supervising the violator shall also be subject to disciplinary actions, in case where the senior employee is recognized to have been negligent in supervision.

② The level of aforementioned disciplinary actions shall be subject to the following standards prescribed in each paragraph.

· Grave Violation (high level)

Breaches stipulated in each of the following subparagraph shall be considered as a "grave

violation."

- In case where the violator inflicted a serious loss to the company's business or damaged the company's reputation.
- In case where the company suffered a serious loss as a result of the violation
- In case where the violation was committed for the purpose of the violator's unfair gains
- In case where the violator leaked information to a competitor or external institution intentionally or without approval from the company.
- In case where dependence with partners or within departments was seriously damaged as a result of violation

· General Violation (mid-level)

- In case where the violator unintentionally inflicted loss to the company
- In case where a hacking incident occurred due to non-compliance with security guidelines

· Minor Violation (low level)

- In case where the breach was unintended or minor, or a simple failure due to the lack of knowledge of security procedures or regulations
- In case where the violation originated from a general practice as a part or whole of the business process
- In case where the volume and content of the leaked information are found to be unimportant as a result of security check

(3) Reinforcement or Mitigation Factors for Disciplinary Actions

The level of disciplinary actions shall be determined with the following factors of reinforcement or mitigation taken into account.

① Reinforcement Factors

· In case where the violator has already been subject to disciplinary actions within the past two years.

· In case where the violator has repeated violation of the same nature two or more times

· In case where it is deemed to need a more serious disciplinary action by the committee

② Mitigation Factors

· In the event of a security incident due to force majeure

· In case where extenuating circumstances exist due to characteristics of the business

· In case where the violator is deemed to have contributed to the interest of the company regardless of the violation

· In case where there may be extenuating circumstances

(4) Specific Standards for Final Judgment

Special cases of violation where it is difficult to apply the above standards on disciplinary actions for violation of information security shall be handled by the Information Security Committee, which shall make a decision on disciplinary actions directly.

Type	Violation	The degree of violation		
		Serious	Common	Light
Personal (Privacy) information	-Leaking, exporting, unauthorized use, destruction, alteration, duplication, copying, concealment, loss of information systems that contain information beyond confidentiality, such as intentional, gross	Dismissal/ Suspension	Suspension/ Wage cut	Wage cut/ Reprimand
	-Leakage, export, unauthorized inquiry, and unauthorized access to information systems that contain information beyond confidentiality, such as personal information, Modulation, lost	Wage cut/ Reprimand	Reprimand/ Warning	Warning/ Caution
	-Unauthorized access and use such as information system bypassing security vulnerability	Wage cut	Reprimand	Warning
	-Violation of compliance obligation of employees	Wage cut/ Reprimand	Reprimand/ Warning	Warning/ Caution

6. Protection of Information Subject

(1) Development and enforcement of response measures to information leakage

① The Company shall notify the leakage of personal information to the subject of information in accordance with relevant laws and regulations without delay upon acquiring knowledge of such accident.

② The Company shall report the leakage of personal information in a certain size defined by relevant laws and regulations without delay upon acquiring knowledge of such accident.

③ Personal information protection officers shall govern affairs associated with protection of the subject of information such as notification or reporting pursuant to relevant laws and regulations, and personal information protection officers may direct relevant departments to protect the subject of information in accordance with the company bylaws and rules on organization and personnel management.

④ Other specific items on the response to any information accident shall be determined by separate guidelines.

(2) Access to personal information by the subject of information

① The Company shall approve access to personal information by the subject of information within 10 days at the request of the subject of information in accordance with the method and

procedures stipulated in relevant laws and regulations, in case where the subject of information requests such access by submitting a request application for access of information.

② The Company may postpone or reject the request for access to personal information by informing the subject of information of the reason, in case where the request falls under reasons for postponement or rejection.

③ The Company shall notify the specifics from Paragraphs 1 and 2 of this Article to the subject of information.

(3) Correction and deletion of personal information

① The Company shall correct or delete personal information within 10 days at the request of the subject of information in accordance with the method and procedures stipulated in relevant laws and regulations, in case where the subject of information requests such correction or deletion by submitting a request application for correction or deletion of information.

② The Company may reject the request for correction or deletion of personal information by informing
the subject of information of the reason for rejection, in case where the request falls under unacceptable reasons in accordance with relevant laws and regulations.

③The Company shall notify the results from Paragraphs 1 and 2 of this Article to the subject of information.

(4) Suspension of personal information management

① The Company shall suspend the management of personal information within 10 days at the request of the subject of information on suspension of management of personal information in accordance with the method and procedures stipulated in relevant laws and regulations, in case where the subject of information request such suspension by submitting a request application for correction or deletion of information.

② The Company may reject the request for suspension of personal information management by informing the subject of information of the reason for suspension, in case where the request falls into unacceptable reasons pursuant to relevant laws and regulations.

③ The Company shall notify the results from Paragraphs 1 and 2 of this Article to the subject of information.

(5) Notification of personal information use

① The Company shall notify the records of personal information use to users on a regular basis, except for cases where it did not collect personal information such as contact numbers.

② The types of information to be notified to users pursuant to the foregoing Paragraph 1 are as

set forth below.

· Purpose of collection and use of personal information and items of collected personal information

· A person provided with personal information, purpose of provision, and items of personal information that has been provided

· A person commissioned to manage personal information and the details of commissioned management tasks

③ Notification pursuant to Article 1 shall be made at least once a year by e-mail, mail, facsimile, telephone or any other similar means of communication.

7. Personal information security training and regular review

(1) Personal information security training

① The Company shall conduct personal information protection training as set forth below to safeguard personal information and prevent any breach of information.

· Frequency of training: at least twice per year

· Subject of training: personal information protection officers, personal information managers

· Content and method of training: education for secure management of personal information and prevention of infringement through a suitable means to a specific situation such as group education, department training, groupware application, etc.

② Personal information protection officers shall maintain material evidence of personal information security training for a minimum of three years.

(2) Enforcement of internal review

① The Company shall enforce an internet review on an annual basis to examine implementation of technical, managerial, physical measures to protect personal information such as access authority management, access history retention and review, data encryption, etc.

② The results of internal review shall be reported to personal information protection officers with potential solutions to any detected problem.

③ The results of internal review shall be shared among employees through regular training sessions, and personal information managers shall take necessary measures to resolve issues including alteration of internal management plan.

④ Personal information managers shall retain the internal review results for a minimum of three years.

(3) External audit

① SFMI conducts audit on information security policies and systems every year by external

institutions such as Korea Financial Security Institute.

8. Miscellaneous provisions

(1) Personal information management and protection organization

General affairs on internal control and protection of personal information shall be governed by the Information Security Department.

(2) Person with Authority

The authority to amend or abolish this policy lies with Chief Information Security Officer (CISO).

It is the principle for SFMI to fulfill the duty of reporting and payment of taxes in an accurate and faithful manner in accordance with tax code and tax rules of individual countries where the company has its presence. To this end, the company has established and managed tax standards for tax-related risk management and disclosed information on tax payment transparently.

Tax Policy

1. Tax Principle

① SFMI shall recognize that compliance with tax code and management of tax risks are critical parts of tax policy.

② SFMI shall comply with tax code and regulations in countries with its business presence and faithfully meet tax obligations including reporting and payment in accordance with relevant laws.

③ SFMI shall not abuse disparities in tax codes of different countries to dodge taxes.

④ SFMI shall not run any legal entity for the purpose of tax avoidance in a tax haven where it is unable to share tax information and the company has no business presence.

⑤ SFMI shall comply with the arm's length principle and have values and commercial substances generated in individual countries adequately allocated as taxable income and shall bear the transfer prices under the arm’s length principle.

⑥ SFMI shall fulfill its duty of tax payment faithfully in accordance with relevant laws and commit its utmost effort to maintain a constructive and transparent relationship with the tax authorities.

2. Tax Guidelines

① SFMI shall record tax reports, evidential documents and materials on tax issues and tax-related decisions in the form of documents.

② SFMI shall monitor amendments to tax codes and new rulings or administrative regulations on tax issues to prevent any potential tax risks.

③ SFMI shall make a decision on tax issues by taking advice from external tax specialists or authoritative interpretations from tax offices, if necessary as to tax issues.

3. Tax Report

① SFMI shall disclose tax payment information through an audit report on DART (Data Analysis,

Retrieval and Transfer) electronic disclosure system of the Korea Financial Supervisory Service.

② Information on the costs and items of corporate taxes shall be provided on the balance sheets of an audit report by an external auditor, with transparency and objectivity assured by an external audit.

③ SFMI shall disclose tax-related information to stakeholders in compliance with tax reporting standards.

④ SFMI shall disclose information on income and tax by country through ESG report every year.

4. SFMI tax policy shall be written based on the review by the tax administrative department and ESG Secretariat. Its content will be reviewed and revised through the ESG Committee on the board of directors and published by an ESG report every year.

SFMI complies with the basic principles on protecting and respecting human rights as outlined in the UN Human Rights Commission's Universal Declaration of Human Rights and Guiding Principles on Business and Human Rights, Korea's Labor Standard Act, and International Labor Organization (ILO) regulations. In addition, principles on the protection of human rights, such as the prohibition of discrimination against employees, respect for diversity, and prohibition of child and forced labor, are stipulated in the Samsung Group's management principle, SFMI's Code of Conduct, and the Code of Conduct for Business Partners, which are observed by all SFMI employees and business partners.

Human Rights Policy

1. Human Rights Protection

① SFMI complies with the regulations regarding working and rest hours and pays wages in accordance with the standards stipulated in relevant laws.

② SFMI strives to create a safe and pleasant working environment for its employees.

③ SFMI pursues a mutually prosperous labor-management relationship based on mutual trust and effective communication.

④ SFMI does not discriminate against employees in terms of working conditions on the basis of their nationality, gender, age, race, religion, or social status.

⑤ SFMI does not allow child labor, forced labor, or wage theft under any circumstances.

⑥ SFMI uses the personal information of customers and employees only for the purpose and through the methods permitted by the laws of each country to protect personal information and performs thorough security control to prevent leakage.

⑦ SFMI respects the dignity of all employees and prohibits inhumane acts such as sexual harassment, corporal punishment, mental or physical coercion, and verbal abuse.

⑧ SFMI shares human rights protection policies with its partners.

⑨ SFMI respects human rights in all of its business activities, including the provision of products and services and investment, monitors major human rights issues, and prepares against potential risks.

2. Human Rights Management

SFMI's commitment to integrating human rights into business management

SFMI and its value chain respect the human rights of all stakeholders in the global market. We observe the UN Human Rights Commission's Universal Declaration of Human Rights and Guiding Principles on Business and Human Rights, the regulations of the International Labor Organization, and the Labor Standard Act of Korea, and signed the UN's Principles for Sustainable Insurance (PSI) Initiative. In addition, we assess the impact of our business activities on human rights in accordance with the Samsung Group's management principles, SFMI's Code of Conduct, and Code of Conduct for Business Partners. We are committed to making improvements and disclosing relevant information.

The Human Rights Policy stipulates the human rights protection principles, including the prohibition of discrimination against employees, respect for diversity, and prohibition of child and forced labor, and describes the patterns of behavior that are necessary to achieve the human rights goals in line with the highest ethical standards. The ESG Committee established in 2021 will adopt the strengthened human rights policy and apply the principles to the company's overall business activities.

3. The purpose and scope of human rights policy

SFMI is doing its best to identify, prevent, and reduce human rights issues that arise in association with our business sites, products and services, business relationships, and projects we have invested in or insurance we have underwritten, and, in turn, directly or indirectly affects our employees, customers, investors, partners, and local communities.

To this end, SFMI engages in the following activities:

- · Raising human rights awareness in all business activities.
- · Communicating with stakeholders to address human rights issues.
- · Adopting grievance handling systems for all stakeholders in relevant countries and departments.
- · Identifying and understanding human rights risks on a regular basis.
- · Addressing the human rights issues that arise in areas we are responsible for and taking corrective measures.
- · Recording the outcome of preventing and addressing human rights issues.

4. Human rights policy for employees

① SFMI respects the dignity of all employees and prohibits all forms of harassment and discrimination on the basis of age, disability, ethnicity, gender, marital status, national origin, political affiliation, race, religion, nationality, sexual orientation, and social status.

② SFMI abides by the regulations on working and rest hours and pays wages in accordance with

relevant regulatory standards.

③ SFMI conducts fair performance evaluations and offers compensations accordingly, and provides employees with equal opportunities for self-development based on their capabilities and talent.

④ SFMI provides and maintains a safe and healthy working environment for all employees.

⑤ SFMI builds a mutually prosperous labor-management relationship based on harmony and mutual trust and respects the employees' freedom of association.

⑥ SFMI operates an official internal reporting channel as part of its effort to practice ethical and compliance management. The identity of reporters and content are kept strictly confidential in accordance with the guidelines on the internal reporting system to make sure all employees and stakeholders can make reports anonymously.

5. Human rights policy for partner companies

① SFMI values its partner companies as business companions and pursues mutual prosperity.

② SFMI established the "Social Responsibility Code of Conduct for Business Partners" and trains, supports, and encourages partners to make improvements in sustainability management in the aspects of human rights, safety, the environment, and ethics.

③ Companies that faithfully abide by domestic and foreign regulations, as well as SFMI's Code of Conduct, are considered preferred potential partners and evaluated accordingly, and the evaluation results are taken into account when the contract is up for renewal.

④ When selecting business partners, we do not force them to purchase our products and services and we engage in transactions as equals.

6. Human rights policy for customers

① SFMI does not discriminate against customers on the basis of gender, age, physical disability, ethnicity, marital status, national origin, political affiliation, race, religion, nationality, sexual orientation, or social status in its provision of financial services.

② SFMI uses the personal information of customers only for the purpose and through the methods permitted by the laws of each country and conducts a rigorous oversight on security management to prevent the leakage of information.

③ SFMI guarantees customers' rights over the control of personal data, as stated in the customer rights notice.

④ SFMI develops and provides the best products and services that meet customers' expectations.

7. Human rights policy for shareholders and investors

① SFMI maintains the accuracy and reliability of accounting data to secure transparency in management.

② Shareholders and investors are provided with the necessary information in a fair and timely manner, in accordance with relevant regulations and internal rules.
③ SFMI builds mutual trust with shareholders and investors by respecting legitimate requests and suggestions.

8. Human rights policy for local communities

① As the number one non-life insurance company in Korea, SFMI is aware of its responsibility for the development of local communities and actively participates in social contribution activities as a member of the community.
② SFMI does not discriminate against the marginalized in society in terms of the provision of financial products and services, employment opportunities, and financial education programs.
③ In the case of large-scale projects that have the potential to cause environmental and social problems, we consider their impact on the local community before making the final decision on whether to provide loans or investment.
④ SFMI strives to create a healthy and transparent society by curbing transactions involving false-name or borrowed-name accounts or illegal money laundering transactions.

9. Human rights policy regarding insurance and investment

SFMI established the ESG guidelines that are applied to insurance underwriting and investment activities. The guidelines prohibit the company from underwriting insurance for policyholders and the insured who have violated human rights, and we do not invest in companies and businesses that are not socially responsible.

SFMI declared "coal free finance" in 2020 to fight against the climate change, which bars the company from not only direct new investment and finance but also investment in corporate bonds for construction of coal related facilities. The company has further integrated ESG elements into its asset management, and has established and managed the responsible investment policy to mitigate the risks of climate change.

Policy on Responsible Investment

1. General Provisions

① SFMI shall live up to the core mission of the property and management industry by playing its role as a social safety net, and execute responsible investment in managing its assets by taking Environment, Social, Governance (ESG) elements into account.

* SFMI carefully considers the definition of each environmental, social, and governance factor. For Environmental factors, we define as responsibilities related to environmental impact, such as environmental protection, climate change strategy, natural environment(world cultural heritage and/or endangered species), and resource usage. Examples include coal infrastructure, coal fired power plants, coal mining facilities, oil sands, and arctic oil fields, among others. For Social factors, we define as social responsibilities related to human resources, product responsibility, human rights, health and safety, inclusive and sustainable finance, supply chain management, information security, and social contribution. For Governance factors, we define as transparency and effective corporate governance, such as ethical management, internal controls, board composition and roles, and accounting and financial management.

② This policy shall define the standards on applicable items and application methods of investment and finance pursuant to corporate regulations.

2. Applicable Items for Responsible Investment

① Investment and loans to enterprises (corporate bonds, bills and loans, stocks)
② Alternative investment, loans (including refinancing)
③ Project funds investing in assets stated above ①~②
④ Blind funds with a specific investment sector or defined business sector

3. Application of Responsible Investment Policy

(1) SFMI shall proactively deliberate on and limit investment and finance in businesses or industries that have negative impact on the environment and society.

① SFMI shall establish standards to exclude coal-related investment from its asset management strategy.

② SFMI may consider influential qualitative information (corporate governance, environmental impact assessment, social impact assessment) and factors contributing to the global society and environmental issues in making investment and financing decisions.

(2) Limited Businesses and Industries

This policy shall be applied to all assets under SFMI management in principle, and the following businesses or industries shall be limited in investment, provided that existing financing shall be redeemed at maturity.

① A company or business related to co al fired power, coal mining, coal infrastructure , tobacco, gambling

② A company or business of which revenue from abovementioned ① accounts for more than 30% of its total revenue, in case where the company runs multiple businesses

③ Other companies or businesses that run counter to the values of social responsibility

(3) Exceptional Cases

① Compani es with energy conversion plans and a company or business of a public nature such as domestic public institution

② Special purpose bonds and funds aligned with the purpose of ESG (green bonds, etc.)

③ Where it meets the K-taxonomy and a certificate meeting the equivalent ESG criteria is issue, etc.

SFMI reinforced insurance underwriting standards for coal related businesses as part of active participation in 2015 Paris Climate Agreement. In 2019, the company factored ESG elements into corporate underwriting strategy, and has since established and managed the ESG insurance underwriting policy .

ESG Insurance Underwriting Policy

1. General Provisions

① SFMI shall implement a policy that factors Environment, Social, Governance (ESG) elements in insurance underwriting, as the company fulfills its role as a social safety net, which is the essence of property and casualty insurance business.

② This policy shall set forth standards for subject matter and method on accepting risks from coal-fired power plants pursuant to SFMI corporate regulations.

2. Underwriting Restrictions

(1) SFMI shall proactively assess and limit underwriting of risks in industries or businesses that has negative impact on the environment and society.

① SFMI shall establish ESG-based underwriting standards on coal-related businesses.

② SFMI may consider factors with environmental impact in insurance underwriting (coal-fired power, LNG gas, petroleum, hydro power, natural resources, etc.)

③ Insurance underwriting includes general insurance and reinsurance. (excluding special reinsurance)

(2) Prohibited Risks

SFMI shall limit underwriting risks for any of the following businesses.

① Coal mining facilities, new coal fired power plants, and new coal infrastructure

② Oil sands / Arctic oil fields and resource development that has a significant impact on the environment, etc.

3. Underwriting Policy Application

① SFMI shall commit to de carbonization in insurance related to coal fired power plants .

② SFMI shall phase in reinforced application of ESG elements in ESG insurance underwriting

③ SFMI shall phase out existing coal related property insurance.

4. Scope of Application

(1) SFMI shall suspend underwriting for the following items pursuant to coal underwriting policy.

① SFMI shall suspend under writing new Construction All Risks (CAR) for coal fired power plants.

② SFMI shall suspend under writing new operational risks for coal fired power plants.

(2) However, the following items may be excluded as exception to the policy.

① Underwriting CAR for the purpose of environmental improvement such as micro dust mitigation

② Exceptions allowed pursuant to national energy policy, considerations of related countries, OECD. arrangements, or other international guidelines

As part of its endeavor to take full responsibility as a global company and help create a sustainable society, SFMI enacted this Code of Conduct guideline which suggests the direction SFMI pursues and specific standards of action that SFMI employees should take.

Code of Conduct

1. Foreword

Socially responsible management by companies has become the central issue for various stakeholders including customers, shareholders, investors, employees, and the government, and it has been building a broad and crucial consensus in the international community. As part of its endeavor to take full responsibility as a global citizen and help create a sustainable society, Samsung Fire & Marine Insurance (SFMI) enacted this Code of Conduct which suggests the direction SFMI pursues and specific standards of action that SFMI employees should take in their work and day-to-day life.

2. Scope of Application

This Code of Conduct shall apply to all current SFMI employees.

3. Use of the Code of Conduct

SFMI employees shall use this Code of Conduct to undertake a preliminary review on the potential impact of their behavior and exert effort to make the right decision in various situations they may encounter as they perform their work. In addition to this Code of Conduct, SFMI employees shall take as references the detailed policies of SFMI business principles and CSR regulations.

4. Internal Reporting Channels

(1) All SFMI employees shall report immediately upon notice any violation of this Code of Conduct or any act suspected of such violation through any of the following channels.

① Whistle-blowing: The Secretariat for Practice of Business Principles (Compliance support part)
- Phone: 02-758-7112
- e-mail: ethics.sfmi@samsungfire.com

② Fraud Reporting: Management Advisory Team
- Phone: 02-758-7106

· e-mail: auditing@samsungfire.com

③ Other violations: ESG Secretariat

· Phone: 02-758-7578

· e-mail: esgnews@samsung.com

(2) The identity of whistle-blowers and detailed information related thereof will be kept strictly confidential, and any act of putting the whistle-blower at risk is prohibited.

(3) SFMI may take a necessary action including imposition of disadvantages on employees who fail to report any illegal or unfair activity that may have grave influence on the Company despite their knowledge of such fact.

5. Protection of Human Rights

(1) Working Environment

① SFMI creates a working environment that promotes employees' autonomy and creativity.

② SFMI has operated and expanded various employee welfare programs to support their work-and-life balance.

③ All SFMI employees respect individual dignity and diversity, follow labor standards and HR regulations for equal employment opportunities, etc. and refrain from any behavior that may harm sound corporate culture including sexual harassment.

(2) Employment Conditions

① SFMI does not discriminate employees on the grounds of nationality, race, sex, religion, age, disabilities etc. with respect to their employment.

③ SFMI provides equal opportunities to employees and treats them fairly based on their capability and performance. SFMI also encourages employees' continued self-development and actively supports their competency improvement.

(3) Resolution of Employee Grievances

① SFMI is committed to listening to employees' suggestions and addressing their issues through consultation and grievance handling systems.

② To develop and maintain w in-win relationship between labor and management based on mutual trust and good faith, SFMI respects employees' freedom of association and rights to collective bargaining and collective action.

(4) Protection of Employee Information

① SFMI protects personal information of incumbent and retired employees.

② An employee's personal information cannot be disclosed without the employee's agreement, barring the following three cases:

· Where it is necessary to comply with special provisions stipulated in the laws and regulations or to fulfill legal obligations

· Where it is necessary for public institutions to perform their duty prescribed in laws and regulations, etc.

· Where it is deemed necessary to protect the physical safety or property interests of the information holder or a third party under the circumstances where the information holder or his/her legal agent cannot provide prior consent or is in a state that he/she is unable to express his/her intent.

(5) Equality and Diversity

① All SFMI employees are respected equally and will not be discriminated based on nationality, race, sex, religion, social status, age, disabilities etc. with respect to the conditions of employment.

(6) Ban on Child Labor and Forced Labor

① SFMI strictly prohibits any forms of forced labor, child labor, and income exploitation.

(7) Sexual Harassment in the Workplace

① Individuals who believe they have been subjected to sexual harassment should immediately report the incident to t heir supervisors, higher management, or their designated Human Resources Department contacts.

② Any forms of harassment including unwelcome verbal or physical advances, coercion of dates by using their positions with the Company, sexually humiliating comments and actions will not be tolerated.

6. Health and Safety

(1) Employee Health and Safety

① SFMI complies with international standards, applicable laws and regulations, internal regulations related to safety. SFMI also endeavors to prevent accidents by following safety rules and creating a healthy work environment.

② SFMI operates Industrial Safety and Health Committee composed of company representatives and employee representatives on a quarterly basis with an aim to enhance employee health

and safety.

③ In order to create a safe working environment, SFMI undertakes periodic safety checks on buildings, electric facilities, fir e prevention systems, and elevators in addition to air quality test, water quality test, etc.

④ SFMI conducts regular and ad-hoc reviews on its buildings under management, including periodic safety checks including regular reviews on seasonal risks such as fire, flood, freeze, rupture, etc. and ad-hoc reviews on decrepit facilities and special medical c heck-ups on workers exposed to hazardous chemicals.

⑤ SFMI has developed and maintained emergency procedures in accordance with the Emergency Response Preparation and Contingency Guidelines to monitor risks such as fire and natural disasters, prevent accidents beforehand, and deal with emergencies.

7. Customer centricity

(1) Marketing and Sales

① SFMI employees are held to the highest standards of business integrity according to SFMI Integrity Sales Practice Code in selling insurance products.

② SFMI employees lead sound sales practices in the insurance business by observing laws and regulations, and exert effort to provide the best in class products catering to the needs of customers. To this end, SFMI employees provides customers with a sufficient explanation on product information and duty of disclosure, and refrain from overstating the features of the products.

(2) Customer-oriented Products and Services

① SFMI prioritizes customer interests by considering from their perspectives, and orients its service systems towards customers. In addition, SFMI embraces customers' ideas and suggestions for improvement and reflect them in various angles from the product and service planning stage. The company also improves product names and policy wordings to enhance customers' understanding.

② SFMI has taken various activities to prevent mis-selling with an aim to establish a culture of trusted Insurance and protect customer rights and interests. To this end, SFMI assigned compliance managers in front offices to operate year-round monitoring and review monthly post-sales mis-selling indexes.

8. Environmental Energy Management

(1) Environmental Safety

① SFMI recognizes its responsibility for the impact of business activities on the environment

including greenhouse gas emissions, and exerts effort to reduce or mitigate such risks on the environment.

② SFMI strives to enhance corporate value in the environment and social sectors by operating enterprise-wide environment and energy management system, and autonomously following international conventions and local environment and energy regulations.

(2) Environment-friendly Products and Services

① SFMI mounts effort to build a sustainable society through insurance and financial product development, risk management and research, and asset management in association with environment and energy conservation.

② When purchasing office supplies including electronic gadgets and stationaries, SFMI puts priority on products with environmentally friendly certificates, recycled products, and highly energy efficient products in accordance with the Guidelines on the Preferential Purchase of Environment-friendly Products enacted in 2006 to promote sustainable purchase.

9. Protection of Information

(1) Prevention of Information Leakage

① SFMI employees shall abide by the corporate process by acquiring approval from the head of their department and IT security department in taking documents, computers, storage devices out of the company premises if necessary to perform company tasks.

② SFMI employees shall comply with the company's internal preliminary approval process in sending out corporate data via email, etc. if necessary to perform company tasks such as writing a report.

③ SFMI employees shall keep confidentiality of the company's business or trade secrets learned or acquired through their positions with the company not only during employment but also after retirement from the company.

④ SFMI employees shall refrain from leaking company information learned or acquired through their positions with the company and other tangible or intangible intellectual assets including trade secrets, classified information on bids, software, and technology development, and personal information of employees without approval from the company. SFMI employees shall refrain from personally retaining company information outside the company premises, and possessing or storing unnecessary personal information in their PCs or drawers.

⑤ SFMI employees shall refrain from leaving in a public places exposed to any third party without encryption resident ID numbers, driving license numbers, passport information, alien registration numbers, or working on physical or electronic documents containing a company password in such public places.

(2) Protection of Customer Information

① SFMI employees shall collect customer information within the scope of business purposes in a reasonable and fair manner, and acquire approval from customers in collecting their information barring exceptional cases stipulated by laws.

② SFMI employees shall comply with legal procedures and methods in accordance with internal guidelines to acquire written approval from customers, and record and maintain the written approval to stay accurate and latest.

③ Customer information shall not be provided to a third party if stated otherwise by law, or granted by customers with their written approval.

④ Customer information shall be retained during a designated period after which it shall be removed in accordance with a legally stipulated method.

(3) Acquisition and Use of Third-party Information

① SFMI employees shall refrain from acquiring trade secrets or classified information of other companies inappropriately, and engaging in or instigating any illegal action to collect important information of competitors.

(4) Management of Information

① For a thorough and rigorous information protection and management, SFMI has designated chief security executive, information security executive, personal information management officer, credit information manager and safeguard. The company also operates the Information Protection Committee composed of top management as a decision-making body on information security issues.

② SFMI strives to protect customer information by reinforcing internal security regulations through a designated organization dedicated to security issues, encrypting customer information and building database with encrypted data, operating information protection system, conducting 24-7 cyber monitoring, separating work network and internet, providing online and offline security education and training, raising employee awareness on security issues and complementing vulnerabilities through mock hacking, undertaking a long term and multi-faceted security review, and strengthening internal control on overall personal information processing and management.

③ SFMI conducts thorough security management and supervision not only on SFMI employees but also on external service providers by establishing a separate security management system for such service providers to ensure that they can safely manage customer information.

(5) Insider Trading

① SFMI employees shall not use or disclose material nonpublic information on the company or a third party for their personal interests.

② Material nonpublic information refers to information disclosed to the general public, which, if disseminated, would likely have a crucial impact on investment decisions including financial information such as profits and dividends and information on organizational change such as merger and acquisition.

③ SFMI strictly prohibits trade of securities based on such material nonpublic information, and SFMI employees shall refrain from making investment into related assets despite their knowledge of such information.

(6) Public Announcement and Social Media Use

① SFMI employees shall refrain from disclosing classified company information in a lecture or interview outside the company without approval from departments concerned.

② SFMI employees shall respect human rights, protect privacy of other persons, and exercise prudence in using social media (SNS, etc.).

③ SFMI employees shall refrain from disseminating unidentified information through social media, and prevent unnecessary dissemination of information pertaining to the company.

④ SFMI employees shall express that their opinions on social media are personal opinions and refrain from suggesting any opinion that may be misconstrued as representing SFMI or SFMI employees.

④ SFMI employees shall refrain from sending out other persons' personal information through social media without their approval and disseminating pornographies, advertisements, or unidentified information.

⑤ SFMI employees shall refrain from exposing information on the company's business affairs or work-related keywords on their social media.

10. Management of Company Assets

(1) Intellectual Property Rights

① SFMI employees strictly comply with laws and internal regulations for the protection of trade secrets and intellectual property rights.

② SFMI employees shall not disclose the Company's trade secrets and classified information, and shall respect intellectual properties of other persons and refrain from acquiring trade secrets inappropriately and engaging in any form of infringement such as illegal copying and distribution.

(2) Company Fund & Asset

① SFMI employees shall use company assets only for public purposes, and acquire prior approval from the head of department if it is necessary to utilize the assets for personal use.

② SFMI employees shall comply with the process when taking company-owned items outside company premises.

③ Any kind of theft or unapproved use of company assets regardless of their residual value on the books, such as tangible assets, scrapped materials, or supplies provided by trading parties is strictly prohibited.

④ SFMI employees shall not use company supplies or remainder of gifts to trading parties for personal purposes.

(3) Conflict of Interests

① It is strictly prohibited that SFMI employees seek personal gains by using Company assets or their positions with the Company and participate in external activities that may cause conflicts of interests, without approval from the Company.

② It is strictly prohibited that SFMI employees seek personal gains by using their titles or positions with the Company or invest in real estates, stocks, etc. under their name or other's name by using the Company's classified information.

③ It is strictly prohibited that SFMI employees acquire Company assets such as vehicles and supplies at a lower price than the market average or sell supplies or amusement park tickets provided for employee welfare purpose by the Company in order to gain proceeds from a third party.

④ It is strictly prohibited that SFMI employees apply for or register a patent developed within the Company personally without approval from the Company.

⑤ It is strictly prohibited that SFMI employees engage in another job without prior approval from the Company or any kinds of activities including side jobs that may harm or interfere with work in the Company.

⑥ It is strictly prohibited that SFMI employees occasionally leave the workplace or attend to personal affairs during working hours without approval from the Company with no justifiable reason.

11. Anti-corruption

(1) Prohibition on Corruption

① SFMI employees shall not provide or receive a gift, entertainment, or courtesy to gain business opportunities or convenience from parties concerned including public officials and customers at home and abroad. SFMI abides by anti-bribery laws of countries around the world and

corporate bylaws on anti-corruption.

(2) Ban on Bribery

① It is strictly prohibited that SFMI employees engage in any kind of activities to seek personal gains unfairly by receiving gift, etc. from companies in a business relationship with SFMI or wishing to develop such relationship.

② It is strictly prohibited that SFMI employees receive from companies in a business relationship with SFMI or wishing to develop such relationship an extravagant golf rounding offer, lavish treatment at a hotel or a fine dining restaurant, or entertainment with alcoholic beverages.

③ It is strictly prohibited that SFMI employees lend money to or borrow money from, demand financial transactions or financial guarantee from, or introduce relatives or acquaintances for the purpose of business deals to companies in a business relationship with SFMI or wishing to develop such relationship.

(3) Ban on solicitation

① SFMI employees shall not cause public officials including non-public officials performing public duties prescribed in the Improper Solicitation and Graft Act to violate laws and regulations or abuse their status and authority in relation to their work stipulated in the Act.

② In relation to the work of public officials prescribed in the Improper Solicitation and Graft Act, SFMI employees shall not provide or promise offering any kind of monetary gift to public officials or their spouses, and even in the case where it is not related to the work of public officials, providing or promising to offer a monetary gift above a limit prescribed in relevant laws is prohibited.

③ It is strictly prohibited to hire employees or condone, incite, or instigate any act of hiring employees in a manner that is not in compliance with the rules of employment or internal regulations and procedures.

(4) Political and Charitable Activities

① SFMI employees respect individuals' voting rights and political opinions, but refrain from engaging in any political activities within the company.

② SFMI employees shall refrain from using financial resources, human resources, or facilities of the Company and offering illegal donations or funds for political purposes.

③ SFMI employees shall refrain from seeking any interest or return for a donation or charitable activity out of the original purpose or making contributions to political candidates and political parties, except as permitted by applicable laws and authorized with the company's prior approval.

(5) Ban on Money-laundering

① SFMI implements Customer Due Diligence (CDD) system in good faith for financial transactions with customers to prevent criminal activities and establish transparent financial market order in accordance with Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) laws. In addition, the Company takes Enhanced Due Diligence (EDD) on the cases classified as high risks in money-laundering risk assessment by transaction type. SFMI operates money laundering risk assessment system for financial transactions to prevent potential risks of money laundering and monitor suspicious transaction reports (STR) and currency transaction reports (CTR). Moreover, the Company strives to make a qualitative improvement in anti-money laundering practices through preventative measures from establishment and enhancement of internal control system to prevent money laundering to occasional review and education programs designed to raise employee awareness and increase employee capability on this matter.

11. Fair Competition

(1) Ban on Monopoly

① SFMI employees respect free and fair market order and abide by fair trade acts of countries around the world.

② SFMI employees compete in a fair manner and capacity, and do not engage in any act that may hinder free competition including collusion with competitors.

③ Any discussion or collusion with competitors over price (premium rate, interest rate, discount/loading rate, etc.), product, underwriting, service conditions, commissions, fees, etc. is strictly prohibited.

(2) Fair Marketing Activities

① SFMI has established and observed the Integrity-based Sales and Marketing Practice Code for business integrity.

② In the case of insurance product sales, SFMI employees shall explain to customers in a faithful manner the essential part of the terms and conditions of a policy including the details of coverage, reason for exclusion, details of interim /maturity refund, etc.

③ SFMI bans any act of promising of additional interest payment or additional coverage out of the scope of product features, as well as insufficient explanation of product details.

④ SFMI bans any act of forcing termination of existing insurance contracts or demanding transfer to another insurance contract after cancellation of a contract.

⑤ SFMI bans any act of promising special benefits or offering premium discounts or other special treatment to insurance policy holders and the insured.

⑥ SFMI bans any act prohibited in the Insurance Business Act in relation to the conclusion and broking of insurance contracts.

(3) Fair Contract

① SFMI employees shall comply with applicable laws and internal regulations in selection of contractors and formation and management of contracts.

② SFMI employees shall not engage in any act to provide special treatment to contractors by using authority given to their positions with the Company in breach of rules and regulations.

(4) Tax Policy

① SFMI complies with laws and regulations based on its internal tax policy, and performs its duty on tax payment on the principle of maintaining an open, honest and transparent relationship with tax authorities.

② SFMI administers financial accounting based on Korea-International Financial Reporting Standards (K-IFRS), Regulation on Supervision of Insurance Business, and other applicable accounting rules. The Company is subjected to regular audits by external experts for financial accounting in accordance with the Act on External Audit of Stock Companies.

③ SFMI faithfully performs its duties pursuant to national accounting laws and regulations and applicable authoritative interpretations including reporting and payment of taxes and submission of various tax reports based on financial information governed by national accounting regulations and internal accounting management system.

④ SFMI rigorously complies with tax laws and regulations in a country with its business presence and fulfills its duty of taxation in good faith.

⑤ SFMI neither exploits the tax table or tax system for the purpose of tax evasion, nor transfers its profits to countries or regions with lower tax rates to reduce the total tax.

⑥ SFMI reviews application of normal price at its overseas subsidiaries in accordance with internal transfer price policy.

⑦ SFMI does not use any tax haven.

⑧ SFMI shall conduct occasional management and monitoring to prevent any other tax risks and transparently disclose tax information in accordance with tax reporting standards.

12. Pursuit of Co-prosperity

(1) Management of Partner Companies

① SFMI recommends that all partner companies adhere to the Code of Conduct for SFMI Partner Companies and requests voluntary agreement from partner companies for compliance with the Code of Conduct.

② SFMI partner companies comply with eight major principles pursuant to the Code of Conduct for SFMI Partner Companies including anti-corruption, observance of laws, ban on child labor, anti-discrimination, accident prevention, disease control, minimization of environment pollution, and protection of the environment.

③ SFMI complies with the Agreement on Ethical Management Practice and conducts monitoring on customer information protection in association with Anycar Lands (SFMI-run car repair shops) and Anycar Family Centers (partnered repair shops). The Company offers various incentives to claims management partners that provide excellent support and cooperation.

④ SFMI reviews the fulfillment of corporate social responsibility by repair shops and partner companies through regular meetings and monitoring, and provides excellent partners with incentives including long-term contracts to ensure that they can continue to reinforce ethical compliance, human rights protection, safety management, and environmental protection.

⑤ SFMI employees respect partner companies as business companions, adhere to laws and regulations on subcontracts, and refrain from abusing their superior status by making unjust demand or taking retaliatory action, etc.

(2) Cooperative Management

① SFMI is committed to enhancing mutual cooperation and creating shared values through diverse communication with partner companies.

(3) Creation of Shared Value

① As a member of local community, SFMI actively participates in resolving various local issues and contributes to enhancing the level of welfare and quality of life in the local community.

② SFMI strives to increase expertise in CSR activities by utilizing the unique characteristics of insurance business and its organizational capacity, and exerts continued effort to help strengthen sustainability of the local community. Moreover, the Company encourages its employees and partners including Risk Consultants (RCs) to participate in volunteering activities and raise donation, while creating synergies with the government and civic organizations through strategic partnerships.

(4) Job Creation and Capability Development

① For economic and social development in the local community, SFMI contributes to job creation and capability development through employment of local residents and provision of education programs.

SFMI developed the "Social Responsibility Code of Conduct for Business Partners" to encourage the practice of social responsibility management and induce change.

Samsung Fire & Marine Insurance Partners Code of Conduct

1. Introduction

Samsung Fire & Marine Insurance enacted the Code of Conduct for Corporate Social Responsibility of Samsung Fire & Marine Insurance Partner Companies to encourage its partner companies to practice corporate social responsibility and bring desirable changes to society. This Code of Conduct recommends responsible business management to SFMI partner companies with regards to ethics, human rights, safety and environment, and all partner companies, suppliers who participates shall comply with this Code. In the event of any conflict between this Code of Conduct and provisions of laws and regulations, more stringent standards shall prevail. This Code of Conduct may be modified in case of any change to partnership management policies of Samsung Fire & Marine Insurance.

2. Human Rights

① Child labor

SFMI partner companies shall prohibit child labor in any case.

② Forced labor

SFMI partner companies shall prohibit forced labor, and any form of labor shall be voluntary. Forced and involuntary labor through confinement contract, exploitation of prisoners, or human trafficking shall be strictly banned.

③ Labor hours and wages

SFMI partner companies shall comply with domestic laws and regulations on working hours and wage. Wage provided to workers shall include minimum wage, overtime allowance, stipulated welfare items, etc.

④ Humane treatment

SFMI partner companies shall not engage in any sexual harassment, sexual assault, corporal punishment, mental or physical coercion, coarse and inhumane treatment involving profanity on employees, nor shall they make any attempt or threat to give such treatment.

⑤ Ban on discrimination

SFMI partner companies shall protect employees from any unfair discrimination caused by bias. In particular, they shall take extra care not to infringe upon the rights of women, children, foreigners, people with disabilities, and those in socially marginalized classes.

3. Safety

① Prevention of accident

SFMI partner companies shall eliminate potential safety risks and take preventive measures to protect employees from any risks. They shall establish and observe procedures to handle contingency cases and tackle accidents in order to minimize damage in case of emergency.

② Disease management

SFMI partner companies shall establish procedures to prevent industrial accidents and occupational illnesses, and provide employees with hygienic working environment including clean drinking water, restrooms, and facilities.

4. Environment

① Minimization of pollution

SFMI partner companies shall observe all applicable laws and regulations on waste disposal to minimize pollution.

② Conservation

SFMI partner companies shall actively engage in environment preservation and promote sustainable resource use through energy conservation, reduction of greenhouse gas emissions, recycling, detection and removal of risk factors, etc.

5. Ethics

① Anti-corruption

SFMI partner companies shall execute all transactions in a fair and transparent manner. They shall not promise, suggest, or offer certain value for the purpose of taking inappropriate gains. Any kind of corruption such as bribery, fraud, money-laundering, embezzlement, concealment, and unfair exercise of influence on counterparties. Accounts, or suppliers shall be completely prohibited, and relevant laws shall be observed.

② Compliance

SFMI partner companies shall not engage in any form of unlawful restrictive business practices such as price-fixing, bid-rigging, and collusive transactions in accordance with Articles 19 and 23 of Monopoly Regulation and Fair Trade Act. They shall also make reasonable effort to protect intellectual property rights, customer information, private information of Samsung Fire & Marine Insurance, and fully comply with relevant laws and regulations.

SFMI is committed to ensuring that customer information is always managed safely by establishing policies on 'customer rights'.

Customer Rights Policy

1. Scope of personal information use for financial services

(1) Your personal credit information is used only for reasons agreed by yourself to settle or maintain financial transactions.

(2) In the process of settling financial transactions or receiving financial services through various channels including front offices and the internet, you may still settle financial transactions or use financial services even if you do not approve that SFMI

① provides your personal credit information (hereinafter "personal information") to partner companies for affiliated or additional services, or

② uses your personal information to introduce financial products or recommend product purchase (hereinafter "marketing" purposes). Without such approval, however, you may not be able to receive affiliated services, additional services, or information on new products and services, etc.

2. Customer rights pursuant to the Credit Information Use and Protection Act

(1) Request for notification of personal information provision to a third-party

① In accordance with Article 35 of to the Credit Information Use and Protection Act, you may request the details of credit information use by SFMI, which has provided your credit information to a third party institution including the Korea Federation of Banks, General Insurance Association of Korea, credit bureaus, and other financial companies.

② How to request

· Mail: SFMI Headquarters (14, Seochodaero 74 gil, Seocho-gu, Seoul) or branch offices

· Phone: 1588-5114

(2) Request for credit information notice for rejected financial transactions

① In accordance with Article 36 of to the Credit Information Use and Protection Act, SFMI may reject or cancel financial transactions with you based on credit delinquency records acquired from financial institutions including the Korea Federation of Banks and credit bureaus. In this

case, you may request SFMI for the name, address, and contact information of the financial institution that provided the credit records as well as the credit information that caused such rejection or cancellation.

(3) Request for suspension of calls or provision of information to third-parties for marketing purposes

① In accordance with Article 37 of to the Credit Information Use and Protection Act, you may request SFMI to stop providing your credit information to third parties or stop calling you for marketing purposes, even if you gave your approval when purchasing a financial product. (However, you cannot demand SFMI to stop providing credit information to the Korea Federation of Banks and credit bureaus for the purpose of credit rating evaluation.)

② How to request

· Mail: SFMI Headquarters (14, Seochodaero 74 gil, Seocho-gu, Seoul) or branch offices

· Phone: 1588-5114

· Internet: http://www.samsungfire.com

③ Restriction

New customers may not be eligible to make such request for the first three months from the date of their financial transactions. However, you can immediately revoke their approval on information use for marketing purposes.

(4) Browsing of personal information and request for correction

① In accordance with Article 38 of to the Credit Information Use and Protection Act, you may request browsing your personal information held by SFMI, and demand correction or deletion of any misinformation. You can make a further request to the Financial Services Commission if you have any objection to the corrected results.

② How to request

· Mail: SFMI Headquarters (14, Seochodaero 74 gil, Seocho-gu, Seoul) or branch offices

· Phone: 1588-5114

· Internet: http://www.samsungfire.com

(5) Request for free browsing of personal information

① In accordance with Article 39 of to the Credit Information Use and Protection Act, you may browse personal information through credit bureaus for free of charge up to a certain times every year. Please make inquiries to the following credit bureaus on the issue.

② Contact

· NICE Credit Information Service Co., Ltd.: ☎ 02-2122-4000 Web site: www.nice.co.kr

· SCI Information Service Inc.: ☎ 02-3445-5000 Web site: www.sci.co.kr
· Korea Credit Bureau Co., Ltd. : ☎ 02-708-6000 Web site:www.kcb4u.com

3. Compensation for damage caused by leak of personal information

In accordance with applicable laws, you may be compensated for any damages caused by leak of personal information attributable to SFMI.

4. If you experience any inconvenience or troubles in exercising the abovementioned rights, please contact the following staff in charge.

① Contact
· SFMI Headquarters for Customer Information Protection and Grievances Resolution:
- Tel: 02-758-7489
- address: 14, Seochodaero 74 gil, Seocho-gu, Seoul
· General Insurance Association of Korea, Personal Credit Information Protection Dept.:
- Tel: 02-3702-8500
- address: F6, 68 Jongro 5 gil, Jongro-gu, Seoul (Susong-dong, KoreanRe Building)
· Financial Supervisory Service Personal Credit Information Protection Dept.
- Tel: Financial Consumer Service Center (without area code) dial 1332
- address: 38 Yeouidaero Yeoungdeungpo-gu, Seoul