Salama Cooperative Insurance Co.
"SALAMA"

Code of Conduct

May 2022

سلامة
SALAMA
شركة سلامة للتأمين التعاوني
SALAMA Cooperative Insurance Company

Document Control

Prepared by	Designation	Date	Signature
Hassan Ahmed Alzahrani	Compliance Manager	04/25/2022	
Reviewed by	**Designation**	**Date**	**Signature**
Abdulrhman Abdullah Alzahrani	Governance Manager	04/25/2022	
Approved by	**Designation**	**Date**	**Signature**
Bader Khalid AlAnzi	CEO	04/25/2022	
Final Approved by	**Designation**	**Date**	**Signature**
Eng. Ahmed Tareq Murad	BOD - Chairman	04/25/2022	

Revision History

Version No.	Date of Implementation	Location of Change	Description of Change
1.0			

1. Introduction

Salama Cooperative Insurance Company (Salama) aims to apply rules of professional conduct to its employees in accordance with the best professional practices in order to provide a moral and professional work environment for its employees. Salama requires its employees to adhere to these rules in order to raise the credibility, efficiency and effectiveness of its activities and maintain its reputation in the financial market.

2. Objectives

The principles of conduct and business ethics in Salama set out in this document are designed to ensure that the performance of the employees of Salama are as per the required ethical values and principles, ensuring work discipline, integrity, transparency, objectivity, efficiency, and effectiveness is reflected in the conduct of Salama employees in performance of their duties.

3. Scope

These principles are approved by the Board of Directors and shall apply to all employees of the company. These principles define the minimum code of conduct for managers within the company who have the responsibility of ensuring the awareness and enabling employees to review and acknowledge the set principles. Managers are responsible for determining whether more detailed instructions or procedures are required within their department to comply with these principles.

4. Purpose

Code of Conduct aims to give employees a structure to follow from the moment they join the Company and making the process of dealing with issues a lot easier as well as setting rules to follow, the Code of Conduct can let employees know what they need to do if they ever need to report a violation of company policy and lets them know the consequences of using false information.

5. Effective Date

The effective date of this policy is from the date of approval from the Board of Directors of Salama.

Note: Any modifications or changes to this policy and to the information it contains should be initiated by the Compliance Officer. Amendments made by any executive power in the company will be considered invalid if not referred to Compliance Department. This document shall be approved by the Chief Executive Officer and Board of Directors of Salama. This document is controlled by the Compliance Officer.

6. Definitions

- Business ethics: A set of ethical standards, rules, and ethics that an employee must have in his profession towards his work, his fellow employees and towards society.

- Company's staff: Board members and committees, executives, employees (officials and contractors), consultants and employees working through a third party.

- Stakeholders: Anyone who has an interest with the company, such as shareholders, creditors, customers, suppliers and any third party.

- Professional conduct: Performing the job duties honestly, impartially, and objectively in accordance with best practices, continuously working to achieve the objectives of the company, and that the practices are within the limits of the powers vested and perform work without negligence and without violating regulations and instructions, and not for the purpose of harming the public interest or to achieve self-interest.

- Internal information: Any information or data or figures or statistics, whether verbal or written or electronic, obtained or reviewed by its employees by virtue of his work or his belonging to the company and which is not available to others.

- Confidential information, data, or documents: Any information or documents that are not publicly available concerning business, administrative and financial arrangements, or the financial position of the company.

- Conflict of interest: A situation in which the objectivity and independence of any of its employees in the performance of his functions is affected by a confirmed material or personal interest that is likely to concern him or one of his acquaintances, or when his performance is influenced by direct or indirect personal considerations by his knowledge of the information relating to the decision.

- Personal Interest: The personal benefit that can be achieved for any of its employees by virtue of the nature of his work or his position and the powers granted to him.

- Disclosure: reporting by the employee to the competent department in the company on the cases identified by the company as requiring disclosure in accordance with the disclosure policy prepared by the company.

- Statutory accountability: holding a person accountable for acts committed by him in violation of the regulations in force and in such a way as to harm others or the interests of the company.

7. Principles of Conduct and Business Ethics

7.1. Integrity and Honesty

The employees of the company shall abide by the following:

- To have the highest ethical standards through transparency, integrity, honesty, and good morals in all dealings with each other and with stakeholders.
- Performing work accurately and objectively in a way that serves the interest of the work and upgrading work skills through continuous education and training.
- Maintaining confidentiality of work by not disclosing any information that may result in a damage to the interest of the company, whether during the period of work or after leaving work.
- Commitment to abiding with the regulations of the Kingdom of Saudi Arabia at all times, training courses and all events and programmes in which the employee represents the company.

7.2. Interaction with stakeholders

Stakeholders have significant importance in Salama and must be treated in a manner that achieves transparency, integrity, and cooperation to the highest professional standards. The policy of the stakeholders prepared by the company determines the general principles and guidelines for their relations with them.

- **Ambition:** The company to be the most trusted and best partner and of best experience for stakeholders by making the business easy and fast.
- **Engagement:** The responsibility of the company towards stakeholders should be providing clear and honest advice and providing the necessary information about products and services to make sound decisions.
- **Response:** The company should give importance to stakeholders' complaints and observations and manage them promptly, effectively, and equitably in accordance with applicable regulations and rules in order to achieve the highest professional standards.
- **Strengthening the principle of trust:** The company should provide clear, understandable, accurate and up-to-date information to stakeholders within the framework of mutual trust in all its services and operations and timely and complete performance of stakeholder services where time is an important component of the company.

7.3. Combating Financial & Administrative Corruption Crimes

- Anti-money laundering, Counter-Terrorist Financing, and Suspicious Transactions
  - Money Laundering and Terrorist Financing are prohibited activities in the Kingdom of Saudi Arabia under the Anti-Money Laundering Law and the Anti-Terrorism Crimes and Financing Regulations and its implementing regulations. Since the effects of those committed crimes do not only affect the company but also affect society and the State. Company employees must combat financial crimes, including money laundering and terrorist financing, and be aware of any unusual or suspicious activities and report them to Compliance and Anti-money Laundering Department in accordance with statutory requirements. It is the responsibility of company's staff to implement the instructions related to AML/CFT, such as reporting suspicious operations and activities and not alerting or hinting to the reported person or any other person that he has been reported. It is the responsibility of the staff of the company to apply the instructions related to combating money laundering and terrorist financing, including the reporting of suspicious operations and activities, and ensuring due confidentiality and privacy. In the event that the communication is found to be invalid, the informant of these instructions and suspicious activities shall not be liable to the informant when reporting in good faith. Suspicious instructions and activities have no liability to the notified when reporting in good faith, the employees assigned to the tasks of AML/CFT are ensured to be adequately equipped with the required knowledge and qualifications.
  - Commitment to the implementation of the Anti-Money Laundering and Anti-Terrorism Financing Regulations and Saudi Central Bank Regulations by the performance of the employee's duties, with honesty, integrity, and professional accuracy to not engage in any criminal activities, money laundering or terrorist financing transactions. The relevant department shall immediately notify the compliance department for combating money laundering and terrorist financing in the company, which in turn informs the General

Directorate of Financial Investigation at Saudi Central Bank of all suspicious transactions made by stakeholders or its employees.

- Not alerting or hinting to stakeholders, affiliates, or others that their activities are under investigation by the Company or have been or will be reported to the competent authorities.

- Anti-bribery and corruption
  - Bribery is one of the greatest crimes and has significant impact on the society. The company condemns corruption and bribery in all its forms and does not accept / tolerate corruption and bribery in any dealings or interaction with stakeholders, and the company is committed to alert and educate its employees on the crime and seriousness of bribery and corruption and its negative damage at the level of Company and community level as a whole. Duties and responsibilities of employees to achieve this includes:
    - Inform the competent directors or departments of the company in case of suspicion of corruption or bribery
    - Not to accept favouritism or intermediary in the performance of work tasks and responsibilities, which may adversely affect the confidence of customers with the company
    - Not to resort to any form of moral or administrative corruption and the use of suspicious or illegal means to accomplish work
    - Not to abuse the functional authority and to inform the competent departments of the company when there is a case of abuse or exploitation.

7.4. Gifts and Hospitality

In the context of relationships gifts and hospitality are offered/accepted, all company employees should exercise caution and apply sound judgment when presenting or accepting gifts from or to stakeholders, to protect the integrity of both the employee and the company in accordance with the policy of gifts and hospitality. To remain mindful of the principles of professionalism, an assessment of whether the gift or hospitality is reasonable, appropriate, and justified taking into account the value, nature and timing of the gift / hospitality and the intended intentions. The staff of the company shall observe the following:

- Not to accept any gift, invitation, service or anything of material or moral value whether it is for him or a relative of a person, or an organization that has a relationship or seeks to have a relationship with the company, so that it can have a direct or indirect impact on objectivity of company employees in carrying out job tasks or may affect their decisions or may compel them to commit to something in return for accepting it.
- Statutory accountability shall be imposed on anyone found guilty of participating, assisting or violating the regulations relating to the request or acceptance of gifts and invitations. This is equal for its present and previous employees.
- If the rejection of the gift would cause offense to the company, or if the refund is not practicable, or provided to the staff of the company on visits and official events or when receiving official guests, which requires the rules of courtesies and protocols of visits and occasions acceptance of the gift may be accepted provided that:
  - They shall not be in cash in any way, or in the form of loans, shares, or financial derivatives.

- The gift and its value should be what is customary to provide, depending on the occasion on which it was presented and its nature.
- If the gift is a reduction or a waiver of fees, it must relate to an invitation to attend a conference or meeting that enhances knowledge and reflects positively on the business of the company and does not result in a conflict of interest.
- The gift must not be related to the position of the recipient of the gift in the company or provided as a result of work in the company.
- The gift holder shall not have a private or public interest, which is requested from the company or one of its employees.

- An employee may accept a prize from other entities that the company deals with as a result of an achievement in the light of the following:
  - The prize should be awarded as part of a declared and recognized program whereby it is awarded on a regular basis.
  - The winners are selected according to a stated criterion.
  - Obtain the prior approval of the company thereof.
- The gift recipient shall present a written disclosure directly to compliance department after receiving the gift in disclosure form in the following cases:
  - If the gift has value and has a price whereby it can be sold.
  - If the gift is perishable and exceeds SR (1000).
- The employees of the company shall be prohibited from giving gifts, grants, and invitations to those who have personal business relationship with the company, unless provided by the competent department in accordance with the policies adopted by the company in this regard.
- It is forbidden to accept or request gifts and grants that have the potential to damage the reputation of the company.

7.5. Compliance with Regulations, Rules, Instructions, and Policies

Adherence to the regulations, instructions and policies is one of the most important factors that enable the company to maintain its reputation and credibility. Employees must adhere to the rules, regulations, instructions, and policies in force related to the work and tasks assigned to them and apply them whilst ensuring that their dealings do not violate any regulations, rules, instructions, or policies relating to the company. Salama employees must ensure that they always take care of the company's interests and not to keep their personal interests over the interests of the Company.

- All Salama employees shall disclose all interests that are inconsistent or possible.
- Employees must ensure that they do not participate in programmes or take decisions that conflict with the interests of the Company.
- Salama employees shall disclose any job vacated during the five years whether or not it was directly or indirectly related to the Company or to any of its work.
- Salama employees shall disclose any other relationship, whatever their nature with persons or institutions related to the Company's activities, including professional relationships as well as direct relationship (parents, children, Wife, brothers and sisters).

- All information disclosed should be sent to Human Resources, Corporate Governance and Compliance Manager to manage compliance and to update this information as soon as any change occurs.
- The Compliance Department must maintain a permanent record of all disclosed information. This information should be kept confidential and not disclosed unless necessary to be disclosed for legal or statutory purposes.

7.6. Dealing with conflict of interest

Dealing with conflict of interest to protect Salama, its employees, are responsible for identifying any potential or actual conflict of interest that could adversely affect the company and/or stakeholders, and in cases where a conflict of interest cannot be prevented, the company manages conflicts of interest through a set of controls, policies, and procedures.

7.7. Maintain confidentiality and information disclosure mechanisms

Information is an important asset for the company's business. Also, its maintenance is deemed as an important element for its success and continuity and all information related to the stakeholders with the company or its employees is deemed as its property. The company has a set of controls and procedures for the destruction of unused or damaged documents and devices

The company classifies the information in terms of confidentiality according to the following:

- Information Classification
    - General Information: Information within the public domain that is freely available to the public through one of the authorized company channels.
    - Internal information: Information not to be disclosed to persons outside the company.
    - Confidential Information: All non-public information related to the company or its employees or stakeholders. Employees of the company familiar with this information must protect it and may only be disclosed to its other employees on a need basis. Unauthorized disclosure of confidential information may result in legal consequences of lawsuits, statutory penalties, or damage to reputation. Examples of confidential information include private information, company strategies, competitively sensitive information, trade secrets, specifications, stakeholder lists or research data. Unauthorized access to this information must be denied.
    - Top Confidential Information: Information that is entrusted to some company employees and which would have a significant impact on the company, its employees or stakeholders if disclosed without permission. The information should be available to employees only as required by the business authorized by the company. Employees must abide by the information security policy, especially those related to dealing with different types of information, and it is strictly forbidden to access information that is highly confidential except for authorized employees.
- Classification of confidentiality

- Confidentiality of stakeholder information: It is the duty and responsibility of the company to protect the confidentiality of stakeholder information. The company's employees are entrusted with important information of stakeholders and this information is important to maintain the company's ability to provide quality products and services. This information includes but is not limited to, personal data, products, services, account transaction balances, private information relating to mergers, acquisitions, and status of securities, as well as related requestor plans to increase capital. According to the strictest confidentiality standards of information, stakeholder information must be treated with the utmost confidentiality. The obligation to maintain the confidentiality of information must continue even after the end of the work / service of the staff of the company, and it is prohibited to share stakeholder information with anyone who does not have access to it from within or outside the company.
- Confidentiality of proprietary information: While working at the company, its employees may provide or develop / access information, ideas, innovations, systems, intellectual property, technologies, policies, procedures, computer operations, equipment, processes , results, profitability forecasts, business plans, strategies, programs, personnel information, reports, studies, records, statements, lists, stakeholder information, trade secrets and other Information relating to the company, its stakeholders, potential stakeholders, its products, services, or any other parties of the company that are not publicly available. Original, copy, electronic, stored, written or any other type, as a condition of employment/service, the company's employees acknowledge that the proprietary information is the property of the company alone and give up any rights or interests to them, as it is the duty of the staff of the company to maintain proprietary information. The employees of the company may not use this information for business other than the company business as well. It is prohibited to make unauthorized use of proprietary information. Employees of the company shall not record any communications involving proprietary information using electronic devices or personal recording devices, including mobile phone cameras. Not to use, divulge or disclose to any unauthorized third party during the period of their work/ service and thereafter. Employees of the company should be careful not to publish or destroy all proprietary information in their possession including those stored in their personal devices and properties such as (electronic devices, PC’s).
- Confidentiality of internal information: Company staff may sometimes be entrusted with internal information that is material. The possession of such kind of information is permitted but it is not permitted to misuse them as the definition of “material internal information” is broad. Internal information is “material” if there is a high probability that an adult will consider it important information to create an investment/business decision or whether the spread of such information will affect the price of the company's securities in the market. Internal information may also be considered material if it relates to the future or

to potential or foreseeable events, or if it is material only if it is combined with information that is publicly available and all information is considered "internal" unless it is disclosed, and the time has elapsed to accommodate it. Examples include the adequate disclosure of information that it provides to securities markets and regulators (such as Tadawul and the Capital Market Authority) or issued in a press release or through meetings with employees of the media and the public. No employee of the company may discuss internal information or pass it on to any other employee unless the exchange of such information serves the purposes of the company. Employees of a company shall not trade directly or indirectly, through a power of attorney or arrange a trading transaction in which one of the parties is a person who relates to an employee of the company by a family, business, contractual relationship or arranges for his agent or another person acting on his behalf in shares or securities to one of the listed companies or gives recommendations to do so based on internal information or sees them by virtue of their work / service in the company. Company employees are not allowed to invest or make business decisions (unrelated to the business of the company) based on information they have obtained from the company. Any such action would be considered illegal and punishable by law. If any employee of the company believes that he has access to internal information, he may not trade securities on the basis of such information, except after consulting the Compliance Department. In case of trading or possessing securities before joining the company, the competent department should be informed.

- Sharing of confidential information based on need: The Company employees should not disclose confidential information to other employees or to supervisory and control authorities, external lawyers and / or consultants, except after obtaining the required approvals according to the following cases:
  - If the recipient has a legitimate need for such information and is licensed to obtain it and is related to the responsibilities of his work in accordance with the governing instructions, no harm will result from disclosure of this information.
  - The Company employees should not give any information about the company to third parties unless they have the authority to do so and there may be an exception to disclose certain information when performing company activities such as solvency inquiries and/or if requested by a supervisory or regulatory body or if disclosure is in the best interest of the company and its stakeholders. However, this exemption will only apply after obtaining the approval of the designated officials of the company.
  - General periodic announcements imposed by regulators if the competent authorities request information for the purpose of investigation.
  - Regulatory and supervisory inquiries should be referred to the Compliance Department. No employee is entitled to respond to any regulatory / supervisory inquiry or provide these entities with any

information required except through the Compliance Department or if they are authorized to do so.

- Duties of company employees:
  - Compliance with the information security policy, procedures, regulations, and instructions related to confidentiality.
  - Not having access to stakeholder or proprietary information that is considered “non-public information” for purposes not relevant to their work.
  - Not to seek confidential information that is not required by their work.
  - Not to provide any unauthorized person from inside or outside the company with confidential information or facilitate access thereto.
  - The authorized persons shall be given the information according to the required limits.
  - Stakeholder information, proprietary information or other confidential information is kept in a way that only authorized employees can access.
  - Do not leave any confidential information in accessible places such as offices or shared places.
  - Use confidential envelopes, postal services or e-mail when exchanging confidential information within the company.
  - Not to take any copies of any document or text, unrelated to their work before obtaining the director's approval.
  - Not to enter lockers, fortified rooms, or other restricted areas unless they are authorized to do so or if it is related to business requirements.
  - Keep documents that are currently working on just above the office and other documents should be kept in the drawers and preferably kept in locked places.
  - Turn off all devices and lock drawers when you leave the office.
  - Destroy all documents that no longer need to be kept and contain sensitive or confidential information. Transactions and other documents are placed in a file inside locked cabinets.
  - Not to disclose any confidential information about the company to any person, including its employees who are not authorized to know this information or employees who do not need such information.
  - Take precautionary measures to avoid unauthorized disclosure of confidential information.
  - Not discuss sensitive or confidential information in public places such as elevators, walkways, and public transport.
  - Maintain the confidentiality of company information during their period of work/service and after the end of that period and not to share another person that information or collect, record or publish at any time for any reason, except after obtaining the written approval of the authorized department within the company.

- Not to enter the building of the company outside the working hours only after obtaining the approval of the Direct Manager and Human Resources Department.
- Understand and acknowledge that any intellectual property developed for the company or created using the resources of the company is the sole property of the company.
- Prevent the disclosure of confidential information, intentionally or unintentionally.
- Adherence to obtain the prior approval of the authorized official to copy or possess any document or text outside the company building to complete work outside the headquarters of the institution.
- The concerned authority of Information Security should be reported if an employee of the company receives confidential information that he does not need. In addition to the above duties, the employees are responsible for the following security obligations:
    - Compliance with the legal requirements and other contractual requirements applied to their job.
    - Maintain Job ID's, confidential numbers of the technical regulations of the company systems considering changing them periodically. Employees of the company are responsible for any work performed under their Job ID's. Information security policies should be followed to prevent misuse of the Job ID's.
    - Not to tamper with the security protection of the technological systems of the company.
    - Take the necessary steps to protect company information stored in computers.
    - Compliance with additional security measures to prevent inadvertent disclosure of confidential information to employees who own laptop computers or who have remote access to the company's systems or who are authorized to use any other portable devices to perform the business of the company.

7.8. Use and release of internal information to manipulate the market/Insider Trading

Employees of the company shall not engage in any act, participate or encourage others in any conduct that may make a false impression of any investment, price or value of something by using or releasing internal information to obtain personal benefits for their own account or for third parties.

7.9. Mechanism for reporting illegal or unethical behaviour (i.e., whistle blowing)

The employee must report cases of fraud or attempted fraud and any loss of amounts or commercial papers or any possible violations of the regulations, rules, instructions and policies of the company. In addition to reporting any unusual transactions, the employee believes that, in his view, they do not correspond to the financial situation of the stakeholders through the different reporting lines provided by the company. The informant on violations shall be dealt with and the company should ensure protection of the

employee reporting the violations. The company should not tolerate any form of reprisals against the whistle blower and hold accountable the employees who deliberately disregard the reporting of any acts or dealings contrary to the relevant regulations, rules, instructions and policies. Further, there is a detailed procedure documented by the Company to deal with whistle blowing cases.

7.10. Rewards and incentives

Salama grants its employees benefits within the scope of their employment contract and in accordance with the approved HR policy, which considers the following:

- Sound and effective risk management through an effective management structure
- Effective remuneration and incentives which is focused on all employees
- Alignment with the company's business strategy, key values, priorities and long-term goals

7.11. Dealing with the press and the media

- The employees of Salama shall not be permitted to declare to the media of any kind or representation (Salama) when participating in conferences and seminars related to the work (Salama) or make any statement or provide information related to Salama's activities before obtaining written approval of the competent authorities of the (Salama), and the authorization is limited to those officially authorized by (Salama), and anyone who provides any information to be aware of its secret nature and that of his authority to declare and deal with it properly.
- Subject to what is stated in paragraph (1) above, it is prohibited to employees (Salama) to provide verbally or in writing an incorrect statement relating to a material occurrence or omission.
- Salama employees are prohibited from promoting, directly or indirectly, an incorrect statement which relates to a material fact, information or opinion with a view to influencing the price or value of a security, or any other goal that involves manipulation.

7.12. Protect the assets of the company

Keep the property of the company and use that very requested property

- Do not use the Company's property for your personal benefit or the benefit of any person other than the Company.
- Use the Company's assets efficiently, for example, telephone or e-mail from your business location is acceptable. However, excessive use of phone calls or e-mail is considered misuse of the property.
- Stealing property of the company, whether theft is taking the company's property, equipment or information without a permit, theft through misappropriation or misrepresentation of expenses - can result in termination of service and legal prosecution. The company also treats theft of property in the workplace that belongs to another employee as theft of the company's property.
- Use of the company's property outside the company's responsibilities - such as the use of business products or use the company's materials or equipment to assist in personal interests. All such acts require prior written consent of the Compliance Department, and

this approval must be renewed annually in case the employee continues to use the property outside of work.

- Salama employees should use their available resources at their disposal for optimal use to achieve its objectives and to preserve their rights and property while carrying out their duties.
- Salama employees must take all necessary precautions to ensure the safety of systems and to protect it from damage and modification.

7.13. Consequences of failure to adhere with the Principles of conduct and business ethics

Salama will ensure the implementation of the Code of Conduct policy, monitor and control any violations thereof and take actions against violator in accordance with the applicable laws and regulations.

7.14. Fair Dealing

The employees of the company shall abide by the following:

- Abstain from any violation of honour and dignity of the job, whether inside or outside the workplace or outside the working hours, refrain from any actions or practices that violate public morals, traditions or customs, and refrain from engaging in political matters or religious or sectarian beliefs of others or incitement against or any form of racism.
- Not to hinder / obstruct the flow of work
- Maintain the reputation of the company by not harming it by publishing information, statements, or comments of its own using various media or communication or by any means or method whatsoever
- Maintain work discipline by abiding with official working hours (official office hours or overtime or official tasks) to perform and complete work tasks
- Be aware of the Regulations and their application without any violation or neglect
- Prior approval should be obtained in the event of public disclosure of information, statements or comments related thereto using various media or communication or any other means
- Optimal and permitted use of the IT infrastructure and technical resources owned by the company in a manner that does not conflict with the workflow

8. Record Retention

SALAMA will comply with the record retention requirements contained in the SAMA and CMA Corporate Governance Regulations and Insurance Market Code of Conduct Regulations and will ensure that all related documentation pertaining to the Code of Conduct are retained for a minimum of 10 years either physically or electronically.

9. Policy review and approval

The Code of Conduct will be reviewed periodically (on an annual basis) or when major changes are warranted or recommended by the Board Audit Committee. The Board is responsible for approving this policy (as required by SAMA).