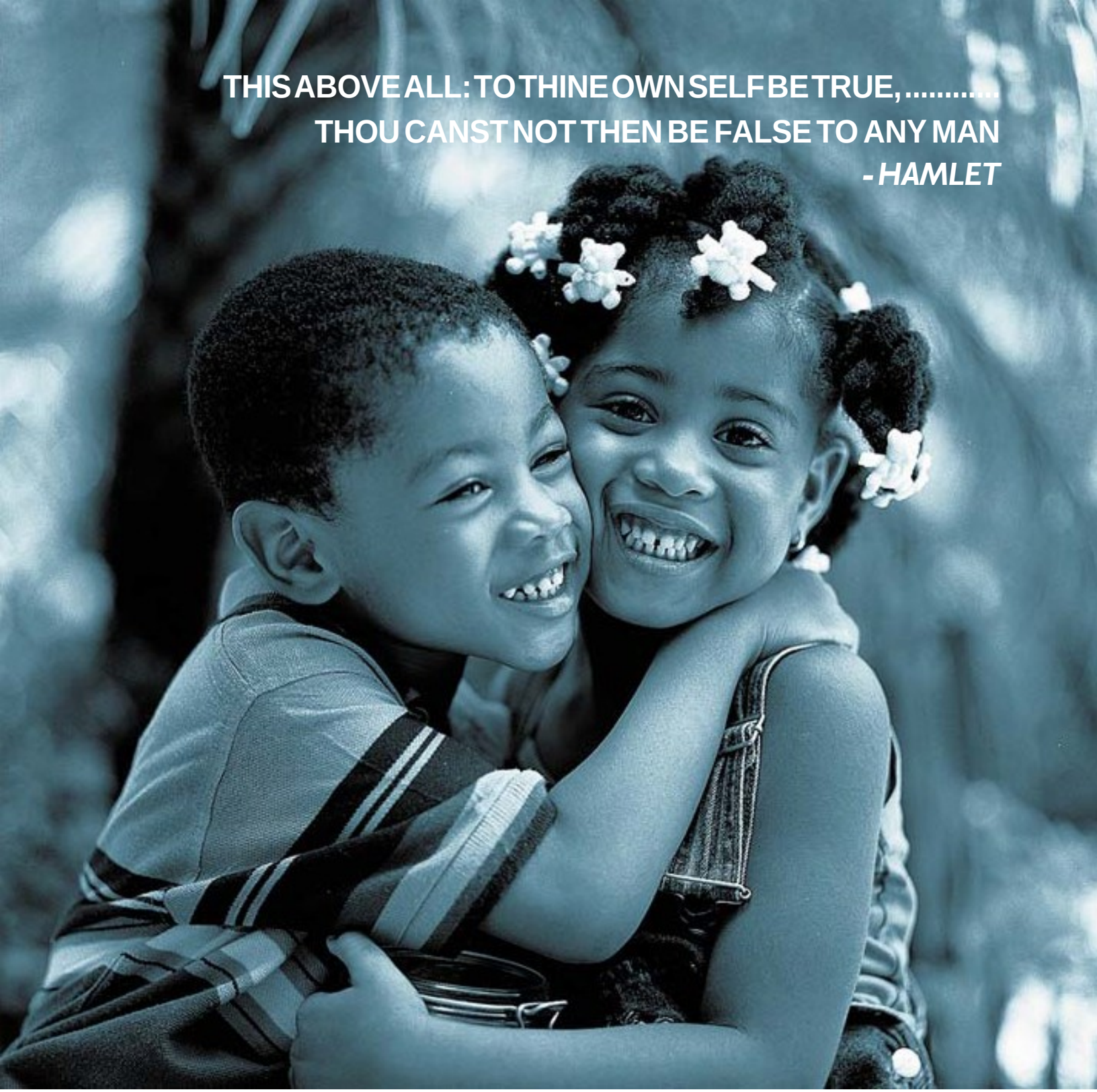


Sagicor

SAGICOR CODE OF BUSINESS CONDUCT AND ETHICS

SAGICOR
CODE OF BUSINESS CONDUCT AND ETHICS

Table of Contents

Message ……..…….. 1

Section A - Overview ……..……..……..……. 2

Section B - Guiding Principles ……..……. 3

1 Duty to Self ……..…….. 3
- 1.1 Personal Integrity ……. 3
- 1.2 Disclosure 4
- 1.3 Professionalism ……..……... 4
- 1.4 Loyalty to the Corporation ……..... 4

2 Duty to Comply with the Law ……..……...… 4
- 2.1 General ……. 4
- 2.2 Inside Information ……... 5
- 2.3 Copyright ……..……... 5
- 2.4 Workplace Health and Safety ……. 6

3 Duty to the Corporation ……. 6
- 3.1 Fiduciary Duty ……..……..…… 6
- 3.2 Duty of Care ……..……... 6
- 3.3 Conflicts of Interest ……..…..……..... 7
- 3.4 Corporate Opportunities ……..……. 8
- 3.5 Disclosure of Outside Information ……..…… 8
- 3.6 Payments, Gifts, Entertainment ……..……..……..… 8
- 3.7 Confidentiality of Company Affairs ……..……..……. 9
- 3.8 Fair Dealing with Suppliers ……..…… 9
- 3.9 Protection and Use of Company Name and Asset …… 10
- 3.10 Directorships in Outside Organizations ……... 10
- 3.11 Fraud and Misconduct ……..……..... 11
- 3.12 Free Competition ……..…… 11

4 Duty to Shareholders and Investors ……..…..… 12
- 4.1 Fair Dealing with Shareholders and Investors ……...…... 12

5 Duty to Customers ……..… 12
- 5.1 Fairness to Customers ……..……..… 12
- 5.2 Confidentiality and Privacy ……..……..... 13
- 5.3 Information Shared with Third Parties …..…….…….... 13
- 5.4 Customer Discrimination ……..... 13

6 Duty to Duty to Employees, Officers, Agents and Directors …… 14
- 6.1 Professional Growth ……..……..…. 14
- 6.2 Reward Performance ……..…….. 14
- 6.3 Privacy and Confidentiality …..…….…….... 14
- 6.4 Liability Insurance ……..……..... 14
- 6.5 Employee Discrimination …..…….…….... 14
- 6.6 Employee Harassment ……. 14

7 Duty to Society ……..……..…… 15
7.1 Political Relations …… 15
7.2 Social Sensitivity ……..……..…….... 15
7.3 Environmental Responsibility ....……..... 15

Section C - Administration of the Code …… 17
1 Introduction ……..……..…… 17
2 Accountability for Code ……. 17
3 Organizational Scope ……. 17
4 Recognizing Breach of Code ……. 18
5 Obligation to Report Code Violations ……..... 18
6 Code Policies, Standards and Procedures …….. 18
7 Code Waivers ……. 19
8 Internal Communications Procedures …… 19
9 Conflict between Code and Local Laws …… 19
10 Annual Acknowledgement ……. 19
11 Availability of Code ……... 19

Document History & Version Control Table

Appendix A – Annual Declaration of Income, Assets & Liabilities form and Internal Disclosure Certificate

Appendix B – Using AlertLine

MESSAGE

To Directors, Officers, Advisors and Employees of the Sagicor Group:

The very essence of the financial services industry demands that we consistently maintain the highest standards of ethical behaviour in dealing with our various stakeholders. In keeping with this objective, the Sagicor Group relies on the single philosophy of "duty" as the cornerstone for the system of ethics and behaviours that guide directors, officers, advisors and employees in the performance of our duties.

We recognize that as a corporate citizen pursuing economic objectives, we are obliged to be respectful of our responsibilities to stakeholders, on behalf of whom this Code has been developed. Such stakeholders include those:

- from whom we obtain the privilege to conduct business;
- who rely on corporate safety, soundness, and profit for the use of their capital;
- whose efforts transform into revenue and profits;
- who buy our products and services in good faith; and
- whose communities we share in the pursuit of our corporate objectives.

The duties above have been formulated into seven Guiding Principles, including the greatest duty of all, the one to self, that as individuals we operate with the highest level of integrity in fulfilling our obligations to those on whom we depend and to others who depend on us. It is this self-respect, more than any written Code of Conduct that has the most powerful influence on an individual's ethical behaviour. My hope is that this Code will define a proper infrastructure of corporate culture that will support people in the full realization of their self-respect and in the consistent practice of ethical conduct.

The Code of Business Conduct and Ethics which has been developed from this simple tenet of "duty" with its seven Guiding Principles is intersected by six core values reflecting Sagicor's commitment to PLEASE:

- **P**rofessionalism
- **L**egal conduct
- **E**thical conduct
- **A**ccountability
- **S**ocial responsibility
- **E**ntrepreneurial leadership

The foremost benefit of compliance with Code standards evolving from the seven Guiding Principles is the personal gratification of doing what is right, followed by the assurance that business obligations to others have been duly fulfilled. On the other hand, the consequences of not complying with a number of the guidelines can be serious, ranging from simple reprimand to fines or even imprisonment.

The reason for such drastic outcomes is simply that as directors, officers, advisors and employees, we all owe a fiduciary duty and a duty of care (statutory obligations) to comply with certain laws. Failure to comply as a result of ignorance or negligence will not absolve us from wrong-doing.

The guidelines that follow are intended to be instructive for guiding behaviour towards doing what is lawful, moral and ethical, with emphasis on deterring wrongdoing that could lead to fraud and misconduct. Several other ethical issues having to do with human resource management, customer relations, etc. have not been included in this Code but are dealt with in internal policies and procedures.

Finally, I doubt very much that we have covered in this Code all ethical scenarios with which you are likely to be confronted. This is neither practical nor necessary but I do sincerely believe that if you internalize the single value of our business "duty" to others and make this your credo, your instincts will guide you towards consistently correct behaviour.

We know we can count on you to do your part; you have our commitment to do the same!

Terrence A Martins
Group Chairman

Dodridge D. Miller
Group President and CEO

SECTION A - OVERVIEW

Sagicor Code of Business Conduct and Ethics ("Code") is intended to govern the behaviour of directors, officers, agents and employees of Sagicor Financial Corporation ("Sagicor", "SFC", "the Company", "the Group") its subsidiaries and controlled affiliates. Third party business associates are also expected to abide by all applicable provisions of the Code and adhere to the principles and values set out in the Code when representing Sagicor to the public or performing service for or on our behalf.

The Code is meant to give assurances to our various stakeholders as to our good intent in the way we conduct business with them. These stakeholders include: shareholders, regulators, customers, suppliers, employees, investors, and communities.

The Code is driven by seven Guiding Principles that reflect the duties we, as directors, officers, agents and employees of the Sagicor Group owe to others in the conduct of our business. The standards contained in this document emphasize deterrence of wrongdoing that could lead to fraud and misconduct, and addresses the following essential areas:

- Conflicts of interest
- Corporate opportunities
- Confidentiality
- Fair dealing
- Protection and use of company assets
- Compliance with laws
- Rules and regulations, including insider trading laws, and
- Encouraging and reporting of any illegal or unethical behaviour.

The individual standards in the Code have been extracted from various internal policies and procedures, which are more comprehensive in detail and procedures for guiding behaviour. References are shown as appropriate within the Code for obtaining additional information.

In Section C you will find guidance for administering the Code, with special emphasis on internal responsibilities, obtaining approvals, reporting irregularities, and escalation. In Appendix A you will find the sample certificate for confirming your compliance with the Code.

Ultimate accountability for the Code rests with the President and CEO of the Sagicor Group, who has delegated responsibility for its administration to the Group Compliance Officer. Outside of their reporting relationships, officers and employees first recourse for seeking approvals and guidance is the Company Compliance Officer; for directors, this resource is the Corporate Governance Committee.

The importance of this Code cannot be overemphasized. You are expected to be thoroughly familiar with its provisions and to conduct yourselves according to both the spirit and letter of the Code. Your cooperation in adhering to the Code is critical to the integrity of our industry and to maintaining the trust that our customers, shareholders, investors and other stakeholders have placed in the Sagicor Group of companies.

SECTION B - GUIDING PRINCIPLES

Seven Guiding Principles evolve from a single concept of duty to those upon whom we depend for the effective conduct of business and to those who depend on us for proper performance.

1. Duty To Self
Directors, officers, advisors and employees owe a duty to themselves for conscionable conduct in the performance of their business responsibilities.

2. Duty To Uphold The Law
Directors, officers, advisors and employees have a personal, civic, and business duty to comply with the law both in letter and spirit.

3. Duty To The Corporation
Directors, officers, advisors and employees owe a moral, ethical and legal duty to act honestly and in good faith with a view to the best interests of the corporation above all other persons.

4. Duty to Shareholders (and Investors)
Directors, officers, advisors and employees owe a duty to shareholders, as owners of the corporation, to maximize the wealth of the corporation for their ultimate benefit.

5. Duty to Customers
Directors, officers, advisors and employees owe a duty to customers to provide them with transparent service solutions that address their real needs and service entitlements, within an institutional environment that protects their confidentiality and privacy.

6. Duty to Employees
Directors, officers, advisors and employees owe a duty to their colleagues to respect their human and civic rights and to enhance their business well-being.

7. Duty to Society
Directors, officers, advisors and employees have a duty to harmonize the operation of the corporation with the aims of communities in which it operates.

1. DUTY TO SELF

Directors, officers, advisors and employees owe a duty to themselves for conscionable conduct in the performance of their business responsibilities.

You have been hired or retained by the Company on the presumption of your high moral character. In your employment with the Company, you are expected always to honour this trust in your integrity and be consistently guided by your conscience for choosing between right and wrong. The judgments you make must be independent of personal interests arising from other business dealings or obligations created by social relationships or personal favours.

1.1 <u>Personal Integrity</u>

The cornerstone of our system of values is the personal integrity of each director, officer, advisor and employee, which collectively defines the institution that we are. As a financial services institution, what we sell is trust, which must be backed by our institutional integrity to deliver. As such, the quality of your response to situations internally and externally must be beyond reproach.

- Know Company policies, rules, and compliance requirements, both internal and external, relating to your work;

- Base your actions on good information and judgment and accept responsibility for outcomes;

- Tell the truth in all communications, making every reasonable effort to provide full, fair, accurate, timely, and understandable disclosure in sales representations and advertising, reports, documents and communications, and avoid errors, omissions, or misunderstandings in statements issued on behalf of the Company;

- Ensure that all transactions, documents, agreements and dealings are recorded and maintained in an accurate and timely manner, and that such records are managed in accordance with records management policies.

- Avoid any conduct or association, either inside or outside of work, which could bring your honesty, integrity or trustworthiness into question, or which could be detrimental to the Company's security or to its reputation within the community.

- Voice concerns when Company policies are not being followed; use the reporting mechanism outlined herein in Section C under the head "Obligation to Report Code Violations".

1.2 Disclosure

Sagicor bestows trust upon its employees and is confident that they will conduct their business with strong ethical commitment, honesty and integrity. Sagicor is required to ensure that it develops a system to evaluate employees' financial history. Having an understanding of employees' financial history will mitigate reputational and regulatory risk which is directly impacted by the reputation and dealings of employees.

You are required to declare your assets, income and liabilities on an annual basis to ensure that Sagicor:

- Complies with regulatory requirements;
- Has knowledge of employees' financial obligations; and
- Is able to evaluate employees' financial history.

Failure to do so could result in significant adverse consequences for the Company directors, officers, advisors and employees

1.3 Professionalism

Professionalism is about achieving excellence in our relations with others. It is about delivering the service and satisfaction that people expect, both in substance and form. It is about our tangible and intangible relations, including those in which we represent the Company externally, what we communicate, how we communicate and how we conduct ourselves in the presence of others. The words we use, our body language, listening skills, appearance and attire all contribute to our professionalism. Not least, the knowledge and skills we apply in the performance of our duties, our timeliness of response, our acceptance of accountability, and generally, our desire to please all reflect our professionalism. Indeed, the level of professionalism we seek in ourselves is a direct outcome of our self-commitment or duty to do the best that we can in the service of others.

1.4 Loyalty to the Corporation

You share responsibility for ensuring that honesty and integrity prevail within the workplace, and for protecting the rights and assets of clients and the reputation of the Company.

- If you become aware of any dishonest, fraudulent, or illegal activities, of any material transaction or relationship that reasonably could be expected to give rise to a conflict of interest, of the falsification of records or returns by another employee, officer, advisor or director, of any breach or

material waiver of this Code of Business Conduct and Ethics, or of any other serious infraction that has occurred either inside or outside the Company, report the matter following the guidelines outlined herein in Section C under the head “Obligation to Report Code Violations”.

- Report also anything unusual that you might notice about a client's affairs that could adversely affect the Company.

2. DUTY TO COMPLY WITH THE LAW

Directors, officers, advisors and employees have a personal, civic, and business duty to comply with the law both in letter and spirit.

2.1 General

The Company’s capacity to do business in its various forms is a privilege bestowed upon it by various Acts, Regulations and Conventions. These privileges remain available to the Company only to the extent that it complies with applicable requirements. Failure to do so could result in significant adverse consequences for the Company directors, officers, advisors and employees.

Company directors, officers, advisors and employees are expected to comply first with the laws, rules and regulations of all countries in which they operate; compliance with the Code is subservient to local laws. These laws include, but are not limited to, company law, insurance laws, investment banking laws, securities laws and regulations, corruption laws, and employment legislation.

- You have an obligation to understand the laws relating to the corporate responsibility assigned to you.

- You are not to take any action that could violate any applicable law, rule or regulation. Seek the advice of internal counsel when in doubt.

- Report promptly to your Manager any actual or contemplated violations of law.

2.2 Inside Information

The nature of your work may cause you to be privy to confidential information concerning the affairs of the Company, a client, a potential client, a supplier, or other company whose securities are publicly traded on a stock exchange. This knowledge is referred to as "inside information" when two specific conditions are met:

- The information has not been generally disclosed to the public, and

- The information is "material" and could have a significant effect on the Company’s investment rating, stock price or securities values.

Inside information might include knowledge of a potential merger or acquisition, a break-through product or technology, significant financial loss or gain, etc. Some Company positions are permanently deemed to be in possession of inside information. The individuals occupying these positions are identified and are under the strictest obligation to observe Company policy regarding the use of inside information.

- You are to scrupulously avoid using, sharing or disclosing non-public information about any SFC company, its subsidiaries, affiliates or clients (both current and prospective), except in the legitimate course of doing business.

- Do not engage in the illegal practice of “tipping” - passing inside information to another person who has no right or need to have it.

- Do not trade in stock or securities, or recommend or advise others to do so, on the basis of inside information you have acquired through your job.

- Before investing in SFC securities, familiarize yourself with Company guidelines on personal trading, including insider trading laws and SFC's securities trading policies, as well as the effect that the perception of wrongdoing may have. If you have any doubts, refer to your immediate superior or to the Company Compliance Officer.

2.3 Copyright

Most printed, broadcast, recorded material or software is protected by copyright laws. The prior approval of the copyright holder may be required before making copies of such material. If in doubt, consult guidelines issued by the Company or seek the advice of your immediate superiors or the Company Compliance Officer.

- Understand and follow the specific terms of any licensing agreement with computer software providers.

- Do not copy any material covered by copyright protection without the prior approval of the copyright holder.

- Do not install or use any software not licensed for use by SFC companies on any company-owned computer.

- Do not copy software programs licensed to SFC companies for use by others, except as permitted by the copyright or licensing agreement. The use of any copies is to strictly comply with the licensing agreement and SFC guidelines.

2.4 Workplace Health and Safety

The Company has a duty to its directors, officers, advisors and employees to ensure a safe and healthy work environment in compliance with laws and regulations and beyond. You have a duty also not to endanger the safety and health of your colleagues through willful or inadvertent acts that expose them to physical harm. Know and observe company policies regarding consumption of alcohol, use of illegal drugs, misuse of premises, verbal abuse, etc. Consult your Human Resource Policy for additional information.

3. DUTY TO THE CORPORATION

Directors, officers, advisors and employees owe a moral, ethical and legal duty to act honestly and in good faith with a view to the best interests of the corporation above all other persons.

3.1 Fiduciary Duty

You owe a fiduciary duty to the corporation to act honestly and in good faith with a view to the best interests of the corporation. (This duty is owed to the corporation as a legal entity and not to individual shareholders.) The obligation to shareholders is a derivative of the reality that the corporation is owned by shareholders, but only to the extent that shareholders' interests coincide with what is in the best interests of the corporation. (In the fiduciary relationship, the beneficiary is the corporation and the fiduciary the directors.) In addition to the fiduciary duty, directors and officers have a duty of care to the corporation.

3.2 Duty of Care

Directors and officers have a statutory duty to exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances. Due diligence refers to the review and investigation directors and officers must apply to situations before reaching a decision with respect to any particular matter. While directors are entitled to rely in good faith on information supplied by management, the duty of care imposed on them requires that they raise questions, follow up, or investigate situations where clarity or sense is reasonably lacking. It is ultimately the director's responsibility to ensure that he/she has the appropriate information necessary to exercise effective business judgment.

- Directors are not to turn a blind eye to an obvious problem in the corporation;

- Directors must apply whatever knowledge, education and experience they have to the business and affairs of the corporation. When particular skills or expertise is required that directors do not have, they are to seek out the experience and expertise of others.

- Directors and officers must avail themselves sufficient time to understand the issues and implications of information supplied to them for decision-making;

- Directors and officers must raise questions and follow up uncertainties, omissions, inconsistencies, and inaccuracies they discern in reports provided them for decision-making;

- Directors and officers must be satisfied that they receive information in a format that allows them to absorb the key issues and reach informed judgments.

3.3 Conflicts of Interest

A "conflict of interest" occurs when an individual's private interest interferes in any way – or even appears to interfere – with the interests of the corporation as a whole." *(Sarbanes-Oxley).* A conflict situation can arise when an employee, officer, agent or director takes actions or has interests that may make it difficult to perform his or her company work objectively and effectively. It is not a question of whether or not specific persons may act inappropriately, only that they are in a situation in which conflict is made possible.

Conflicts of interest damage the trust between you, the public and the Company. Even the appearance of a conflict may be harmful to the Company. Generally, avoid situations in which you or anyone personally associated with you, including friends and relatives, are exposed to self-enrichment at the expense of the Company.

- Directors shall declare their interest in any matter coming to the board for decision and shall not participate in debate or vote on such matter, unless otherwise approved by the Board.

- Any waiver of the Code for executive officers or directors is to be made only by the board and must be promptly disclosed to shareholders.

- Officers and directors shall not waive conflict of interest guidelines unless they have fully applied their duty of care and due diligence to satisfy themselves that the interests of the Company are not likely to be compromised.

- Any waiver of the Code must be accompanied by appropriate controls designed to protect the Company.

- Do not make a material investment in a business entity with or in which the Company transacts business or is considering making, intends to make, or has made an investment.

- Do not enter into any contract or transaction, directly or indirectly, for the provision of goods or services with the Company unless:

    - You have disclosed the situation in writing to the corporation;

    - You do not occupy (in the corporation) a position that makes decisions for the procurement or use of the goods or services, or that is responsible for accounting entries;

    - The situation is clearly fair and reasonable from the corporation's perspective at the outset;

    - Officers, advisors and employees obtain approval in writing for the contract or transaction;

    - The director abstains from participation in debate and voting on any resolution to approve the contract or transaction.

- Do not make any significant investment in any competitor, supplier or customer of the Company that could interfere with your objectivity or commitment in the performance of your duties with SFC.

- Do not approve a loan, any other product, service request or transaction for yourself or for any client with whom you are personally associated, including friends and relatives. These situations are to be referred to your manager.

- Officers, advisors, employees or members of their immediate family are not to acquire any assets or property from a client's estate, either directly or indirectly, nor accept executorships (paid or unpaid) for the settling of a client's estate, unless you can clearly demonstrate that the assets, property or executorship appointment are totally independent of your employment status.

- You may, subject to prior approval by the Company, accept other employment while employed by a SFC company providing it:
    - is legal;
    - is not with a competitor;
    - does not expose you to a conflict of interest; or
    - will not interfere with the your work performance in SFC.
- You may work in the same unit or department with someone with whom you are personally associated, including friends and relatives, providing there is no conflict of interest, there is not a reporting relationship, and the work arrangement does not result in a potential security risk.

3.4 Corporate Opportunities

Arising from their inner familiarity with the corporation's business and dealings, directors, officers, advisors and employees are in a position to learn of economic opportunities available to or being contemplated by the corporation, creating the real possibility that they may usurp the corporate opportunity. On the other hand, employees, officers and directors owe a duty to the Company to advance its legitimate interests when the opportunity to do so arises.

- Do not appropriate for yourself economic opportunities discovered through the use of corporate property, information, or position.
- Do not use corporate property, information, or position for personal gain;
- Do not use corporate property, information, or position to compete with the Company.

For example, if Sagicor is considering investing in a particular business, you may not use the knowledge of that opportunity acquired as a result of your relationship with Sagicor to take that opportunity away from the corporation and make the investment yourself.

3.5 Disclosure of Outside Information

As fiduciaries, directors and officers have an obligation to disclose to Sagicor any information in their possession that may affect "a vital aspect of its business". Officers and directors will not be conducting their relationship with the Company in good faith while having in their possession information about events and situations which could have a material adverse impact on the Company.

3.6 Payments, Gifts, Entertainment

You are encouraged to consider the motive behind business gifts and entertainment to yourselves or family and to ensure that these are given only in the spirit of business courtesy and relationship management and not to set up reciprocal expectations of business favour. As a guide, a modest value of approximately US $100 (or equivalent value) should be applied in assessing what is reasonable to accept. If in doubt, as to what is considered acceptable to give or to receive, seek guidance from your manager.

- You are not to be involved in any act that could be interpreted as seeking, receiving or dispensing a bribe, kickback or questionable payment;
- You may supply or accept modest gifts, favours, entertainment or services provided they:
    - do not consist of cash, bonds, or negotiable securities;
    - are unlikely to be interpreted as a bribe or other improper payment;

- conform with generally accepted ethical and legal standards as well as public disclosure requirements;

- will not embarrass the Company or the recipient.

3.7 Confidentiality of Company Affairs

Your fiduciary duty requires that you protect information about the Company which is confidential or proprietary to the corporation and which could be useful to competitors and harmful to the Company or its customers. This is intended to prevent those competitors from having access to such information and using it to their own advantage at the corporation's expense. Confidential information includes: business plans, business forecasts, strategic initiatives, proposed acquisitions or divestitures, and current or proposed products.

You are responsible for protecting confidential information in your possession against theft, loss, unauthorized disclosure, access or destruction, or other misuse.

- Only disclose confidential information to others within the Company on a need-to-know basis or when authorized to do so.

- Control access to confidential information, for example, by not leaving it unattended in a conference room or discarding it in a public place.

- Exercise discretion when discussing company business especially in public places such as restaurants, airplanes, over public or mobile phones, the internet and fax machines.

- Do not disclose corporate information to outsiders, even if the outsider is a business associate, client, or customer of yours, as you are bound by a fiduciary duty not to do so.

- Extend the use of confidentiality agreements to part-time, temporary and contract employees, consultants, and vendors to the extent that they have access to confidential corporate information.

- Do not remove any proprietary information from company premises without permission from your manager.

- Do not give testimony about the Company or general industry policies or business practices in a court of law in matters not involving SFC as a party without prior authorization from Sagicor's legal counsel.

- Should you leave the service of a SFC Company, you are obliged to continue safeguarding for an indefinite period of time the privacy and confidentiality of the affairs of the Company, clients, directors, officers, advisors and employees. Specific client information – including names, lists, profiles, data, etc. – is not to be used in subsequent employment situations. Any client or proprietary information you have in your possession is to be returned to the organization when you leave the Company's employment.

You must also comply with the requirements related to the confidentiality of material non-public information contained in the Insider Trading Policy.

(These confidentiality provisions are in addition to those contained in Section 5 below, "Confidentiality and Privacy".)

3.8 Fair Dealing with Suppliers

Each director, officer, agent and employee must endeavour to deal fairly with the Company's suppliers. You should not take unfair advantage of suppliers through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practice.

Sagicor is committed to fair competition in all its dealings with suppliers, who are generally chosen on the basis of merit, competitiveness, price, reliability and reputation.

- You must not be associated in any way with agreements between the Company and suppliers in which you or a member of your immediate family have an interest or which might result in your or your family member's personal gain.

- For relatively large contracts, use a bidding process and a committee assessment approach for choosing suppliers;

- Do not endorse a supplier's product or service using the Company name without approval from the Company Compliance Officer.

- Do not suggest or imply to a supplier that the Company's patronage depends on the supplier becoming a customer of the Company, or on the supplier continuing to do business with the Company.

3.9 Protection and Use of Company Name and Assets

All employees, advisors, officers and directors have a duty to protect Company assets and ensure their efficient use for legitimate business purposes only.

- The name "Sagicor" or any parts thereof, is to be used only for authorized company business and never for personal activities.

- Do not identify yourself with the Company while pursuing personal, political or not-for-profit activities, unless you obtain prior Company approval.

- Ensure that each use, acquisition or disposition of an asset by a person on behalf of the Company is undertaken with the general or specific authorization of management and is accurately and fairly recorded in reasonable detail in the Company's books of account and record.

- Company time, real property, intellectual property, financial assets, equipment, services, stationery, computers, communication equipment, and mail services are not to be employed in personal or non-business uses.

- You may not remove or borrow any Company asset without prior and proper permission.

3.10 Directorships in Outside Organizations

Employees and directors who are invited to sit on the boards of external organizations or to accept other appointments may do so, providing they observe the established SFC guidelines. Keep in mind that accepting directorships in other entities may not only compromise your loyalty but demand of your time. In any event:

- Executives who are directors are not to hold more than one other significant external appointment or directorship. Consideration of such appointment is to be discussed with the Group President and CEO and Board Chairman and approved by the Board. (Unless the external appointment is taken up at the Company's request, it is usual for the Director concerned to retain the fees for such external appointment.)

- An executive who is a director is not to accept an appointment as a non-executive director of any other company where a Sagicor non-executive director is an executive director.

- For publicly traded, private for-profit, or venture capital entities/organizations, even where the organization or entity is connected to a SFC company, refer to policy guidelines for required process and approvals.

- For not-for-profit organizations, obtain executive approval from the officer responsible for your unit or function.

- If you are a member of a public or quasi-public decision-making body such as a school board or town council, you should recognize that these institutions are often consumers of financial services and may be actual or potential clients of SFC companies. You are cautioned to assess the potential for a conflict of interest before accepting, and

    - declare any such conflict to the institution and your manager;

    - avoid being caught in situations where you are required to exercise judgment with respect to Sagicor's affairs.

3.11 Fraud and Misconduct

The fiduciary duty is imposed on every director, officer, advisor and employee to ensure that you are acting honestly and in good faith with a view to the best interests of the corporation, regardless of how colleagues may conduct themselves.

- The funds, property, information and services entrusted to our care belong to the Company and their clients alone. Using these assets carelessly, inappropriately, or for personal gain is a violation of this trust.

- SFC Companies are obliged to safeguard the assets of their clients and member companies at all times, and to protect them from all forms of misuse.

- You must not, under any circumstances, misappropriate funds, property or other assets, or knowingly assist another individual to do so. (Misappropriation includes theft, fraud, embezzlement, unauthorized "borrowing", or "kiting" (taking advantage through any means of the time delay required for a cheque to clear at one financial institution and be charged back to another).

- You are not to convert any assets that do not belong to you, or use them for the benefit of yourself or anyone other than the rightful owners. You are not to knowingly assist another in this pursuit.

- If you have access to a Company expense account, you are to claim only those expenses that are eligible for reimbursement under Sagicor's expense guidelines. Intentional use of expense accounts for personal purposes represents misappropriation of company funds.

- Do not compete with the Company.

3.12 Free Competition

SFC companies are committed to free competition and do not support any agreements, actions or concerted practices that restrict or impede fair competition.

- Avoid any collusive, anti-competitive discussions and/or agreements with competitors, especially on pricing, product offerings, and target markets.

- Do not malign competitors; instead, promote the strengths of your own Company;

- Benchmarking with a competitor may be risky; obtain prior business and legal approval;

- Avoid discussing sensitive topics like price, costs, or marketing plans at trade associations or seminars.

4. DUTY TO SHAREHOLDERS AND INVESTORS

Directors, officers, advisors and employees owe a duty to shareholders, as owners of the corporation, to maximize the wealth of the Corporation for their ultimate benefit.

The board has a business duty to provide leadership to the corporation for maximizing shareholder wealth, or at least to preserve wealth, i.e. to ensure it is not dissipated. The board fulfills this duty by carrying out its responsibilities in accordance with statutory, regulatory and best practice requirements and with due regard to prudent risk management.

- Directors must supervise the management of the corporation and provide leadership such that its wealth is preserved if not maximized;

- Directors must put the interests of shareholders before all others in the normal course of the Company's operation, except that laws and ethical behaviour are not to be compromised.

4.1 Fair Dealing with Shareholders and Investors

Shareholders and investors invest in SFC accepting a certain risk-reward at the time of their investment. If the Company's risk profile changes or is likely to change in a material way, especially arising out of corporate action, they are entitled to be informed to afford them the opportunity to react to such information.

- Financial statements must be prepared in accordance with generally accepted accounting principles, including the accounting requirements of applicable regulators. The Company's financial statements must fairly present, in all material respects, the financial position, results of operations and cash flows of the Company.

- Directors must provide shareholders with timely and full disclosure of all events which affect or are likely to affect the board's ability to discharge its fiduciary duty and duty of care;

- Directors must provide shareholders with timely, full and accurate disclosure of all events or situations that have or are likely to have a material adverse impact on the corporation's risk profile.

- It is unethical and illegal for directors, officers, advisors and employees to buy or sell SFC securities with the benefit of material information that has not been publicly disclosed about the Company or its affiliates, or to inform any other person, except as permitted by law, of material information that has not been publicly disclosed.

- It is unethical and likely illegal, to buy or sell securities of another company based on your knowledge of Sagicor's investment intentions or on any material information about the other company that has not been disclosed.

5. DUTY TO CUSTOMERS

Directors, officers, advisors and employees owe a duty to customers to provide them with transparent service solutions that address their real needs and service entitlements, within an institutional environment that protects their confidentiality and privacy.

5.1 Fairness to Customers

It is our ethical responsibility to treat customers fairly in all our dealings.

- Honour our claims payment obligations.

- Communicate only factual advertising and use only easy to understand sales materials based on the principles of fair dealing and good faith. All promotional efforts, illustrations of products and marketing concepts must be factual.

- Use only fair and honest sales and negotiating methods. Never make statements about competitors that are untrue nor make statements about the Company that are untrue.

- Avoid any sales practices that could be misconstrued as an attempt to impose undue pressure on or to coerce a client into obtaining a product or service from a SFC company as a condition of closing a sale ("tie-in" selling).

5.2 Confidentiality and Privacy

Customers have a moral and in some cases, legal right to privacy and to the security of their personal information as a condition of doing business with us and you must respect and preserve this right. Our reputation depends on how well we honour the trust placed in us by customers and it is essential that we maintain this trust through consistent observance of applicable privacy and confidentiality rules.

- You are to comply at all times with the applicable policy relating to client privacy and respect the confidentiality of client information.

- If, in your position, you have access to client information from more than one SFC company, you are to ensure that proper client consent is in place before sharing that information with member companies.

- Should you leave the service of a SFC company, you are obliged to continue safeguarding client privacy and confidentiality, including names, lists, profiles, data, etc. Any client or proprietary information you have in your possession is to be returned to the organization when you leave.

(These confidentiality provisions are in addition to those covered under "Confidentiality of Corporate Affairs" in Section 3 above.)

5.3 Information Shared with Third Parties

In the course of regular business activities, SFC companies frequently enter into contracts with a variety of outside parties including vendors, suppliers, service providers, etc., often resulting in the exchange of information.

- Share Restricted, Confidential or SFC Internal information only with third parties who have undertaken in writing to keep the information confidential in accordance with Company requirements.

- Share only that information which is needed to satisfy the conditions of the contract and only with those who need to know.

- Do not share any confidential information about an outside party (vendor, supplier, service provider, etc.) except to satisfy the obligations outlined in the contract and only to those who need to know.

5.4 Customer Discrimination

Service is to be rendered to customers without prejudice or discrimination on any grounds, including race, colour, religion/creed, age, gender, marital status, sexual orientation, disability, or political affiliation. Customers have both a legal and moral right not to be discriminated against.

6. DUTY TO EMPLOYEES, OFFICERS, ADVISORS AND DIRECTORS

Directors, officers, advisors and employees owe a duty to their colleagues to respect their human and civic rights and to enhance their business well-being.

Recognizing that the business organization is a social system of individuals with various aspirations, backgrounds and divergent sensitivities, we strive to provide an organizational environment conducive to personal growth and satisfaction. Within our organizational community, we have a duty to be respectful to each other foremost in terms of our human rights and needs and next as employees with objective roles and responsibilities.

6.1 Professional Growth

We have a business and ethical duty to our directors, officers, advisors and employees to provide them with challenging work experiences and to facilitate development of their skills to enable them to actualize their potential for personal growth and ultimate business performance.

6.2 Reward Performance

As a performance-oriented Company, we place a high premium on achievement and encourage superior performance through structured financial rewards.

6.3 Privacy and Confidentiality

Most directors, officers, advisors and employees have both a business and customer relationship with SFC companies. Personal information about you as a client is confidential and is treated in the same manner as any other client. As with any other client, cross-referrals or product/service promotions require your prior written consent. Similarly, personal information about you as an employee and director is confidential. Any sharing or use of this information for client-related purposes needs your prior consent.

- Any inquiries you may receive about an employee, officer, agent or director or requests for their information – including those concerning former employees, officers, agents and directors – is to be handled in strict compliance with applicable privacy policy.

- Should you leave the service of a SFC company, you are obliged to continue safeguarding director, officer, agent and employee privacy and confidentiality.

6.4 Liability Insurance

The Company has an ethical responsibility to its directors, officers and employees to defend them, or reimburse costs incurred in defending themselves, against wrongful legal action relating to the performance of their corporate duties. Each situation will be judged on its merits.

6.5 Employee Discrimination

SFC companies are committed to promoting and upholding equal opportunity in all dealings with employees, officers, agents and directors, who have a moral and legal claim to such treatment.

- Do not practice prejudice or discrimination towards your colleagues on any grounds, including race, colour, religion/creed, age, gender, marital status, sexual orientation, disability, or political affiliation.

- Do not engage in discriminatory practices that are contrary to the principles established for SFC companies.

6.6 Employee Harassment

Employees, officers, advisors and directors have every right to work in an environment that is free from harassment. Harassment involves conduct that interferes with a climate of understanding and a mutual

respect for the dignity and worth of each person. It undermines the integrity of the employment relationship, erodes morale and interferes with the productivity of its victims and their co-workers.

Under no circumstances are you to engage in behaviour which is known, or should be reasonably known to be offensive or harassing. Please refer to Company HR Policy for more specific guidance and procedures regarding employee harassment.

7. DUTY TO SOCIETY

Directors, officers, advisors and employees have a duty to harmonize the operation of the Company with the aims of communities in which it operates.

It is our duty as a corporate citizen not to deplete society's resources in the pursuit of corporate objectives but on the other hand, to add value to community life while earning a profit for our shareholders. SFC companies take responsibility for the effects of their actions, both social and economic.

7.1 Political Relations

SFC companies will make only those contributions permitted by law to a political party, candidate, or campaign and only as an expression of responsible citizenship – not to "purchase" favours or to gain improper advantage. Contributions to political parties, constituencies, and candidates are not included in the corporate philanthropy program.

- You are encouraged to take your civic responsibilities seriously and participate in general political processes such as school board, and local and national elections.

- You are not to make political contributions in the name of a SFC company unless you are specifically and explicitly mandated by the Company to do so.

- Do not provide gifts, entertainment, or other gratuities to any government official without first consulting with your executive head or Company Compliance Officer.

- Do not give anything of value to employees or representatives of foreign governments or governmental agencies, political parties, or political candidates to influence a foreign official in the performance of official duties.

- Should you choose to become involved in political activity, you do so on your own behalf and not as a representative of SFC. You are not, in any way, to use your affiliation with the Company in promoting yourself.

- Do not make available the use of Company facilities, including office space and equipment, as well as the donation of the services of Company employees to the campaign committee of a candidate.

7.2 Social Sensitivity

SFC companies accept responsibility and are accountable for the social and economic effects of their business actions and decisions.

- Consistently evaluate the likely implications on society of broad actions you take regarding investments, hours of business, dis-investments, etc.

7.3 Environmental Responsibility

SFC companies are dedicated to protecting and enhancing human health, natural resources, and the environment. This commitment reaches beyond compliance with the law as SFC companies will play a leading role to educate the public regarding environmental protection and to support activism in this regard.

- Conduct business operations in a fashion that ensures environmental laws and standards are met or exceeded.

- Support the efforts of communities to enhance and protect their natural environment.

SECTION C - ADMINISTRATION OF THE CODE

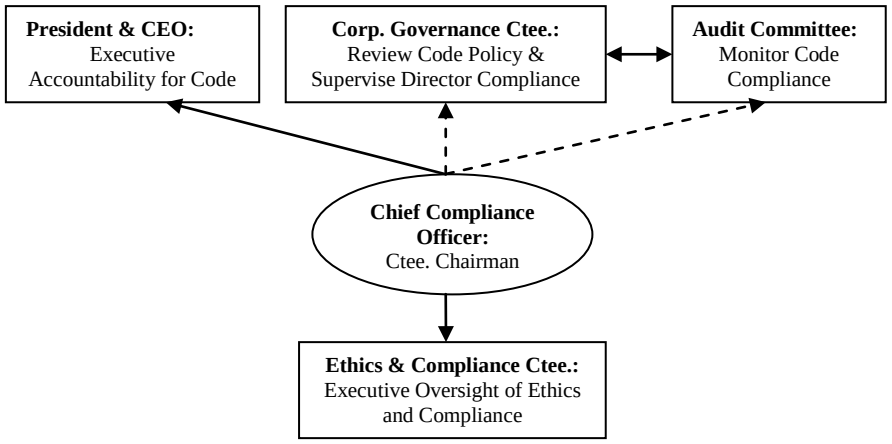
1 Introduction

The guidelines that follow are intended to:

- Describe how the Code is implemented.
- Describe how directors, officers, advisors and employees may respond to the Code, particularly with respect to reporting and escalating issues.
- Describe how the board monitors or satisfies itself regarding compliance with the Code.
- Disclose how a person or company may obtain a copy of the Code.

2 Accountability for Code

Ultimate accountability for the Code rests with the President and CEO of the Sagicor Group, who has delegated responsibility for its administration to the Group Compliance Officer. The GCO chairs a management committee, Ethics and Compliance Committee, approved by the board to oversee administration of ethics and compliance throughout the Group. Committee responsibilities include coordinating ethics and compliance policy, organization, execution, reporting throughout the group, and reporting to applicable board committees.



3 Organizational Scope

This Code of Business Conduct and Ethics ("Code") applies equally to all directors, officers, advisors and employees throughout the Sagicor Group, including subsidiaries and controlled affiliates. Third party business associates are also expected to abide by all applicable provisions of the Code and adhere to the principles and values set out in the Code when representing Sagicor. The Code is intended to give assurances to our stakeholders, including shareholders, investors, lenders, partners, associates, customers/clients, employees, suppliers, regulators and the communities we serve.

"Sagicor Financial Corporation", "Sagicor", "Sagicor Group", "SFC" and "Company" all have the same meaning in this Code. The Code is available on the Company's web site and is also available in print upon request.

4 Recognizing Breach of Code

If you are in doubt as to whether you or someone else is in breach of the Code with respect to any particular situation, apply the following questions to assist you in reaching a decision:

- How would I feel about myself if I did this?
- How would I feel if someone did this to me or my company?
- Is the action fair or ethical? Is it legal?
- How would I advise a young person to act in this situation?
- Would the Company be likely to lose customers or shareholders if this action were known to them?

5 Obligation to Report Code Violations

You must promptly report any known or suspected breach of this Code, any applicable law or regulation or external code of conduct, standard or guideline, whether by yourself or someone else. If you are an officer, advisor or an employee, you should report any breach or suspected breach to your immediate Manager. If you are a director, you should report any breach or suspected breach to the Chairman of the Board or to the Chairman of the Corporate Governance Committee. If you are a Manager, you have the same reporting responsibility as your subordinate employees and shall report all cases of violations or suspected violations within your personal knowledge as well as those reported to you by your subordinates to the Company Compliance officer. If you are a Company Compliance Officer, upon receipt of a report under this Code, you shall forthwith notify the Group Compliance Officer, the Chief Internal Auditor, the local HR department and the Assistant Vice President, Legal and Compliance, Sagicor Financial Corporation. In addition, you should report as provided above if you become aware of or suspect illegal or unethical conduct by any of the Company's clients or third party business associates that may affect our business relationship with them or the Company's reputation. The Company will respect the confidentiality of those who report a concern and will not divulge the reporter's identity without his/her consent.

You may also choose to report any concern anonymously to Sagicor's management via telephone or the internet. Such anonymous reporting is facilitated through an independent third party service called "AlertLine". Reports may be made via this facility in complete anonymity 24 hours a day, 7 days a week by calling the toll free number 1-(888) 307-5991 or by logging on to http://www.sagicor.alertline.com. Details relating to the use of the AlertLine facility are contained in Appendix B hereto. Please be aware that the Company's ability to fully investigate an anonymous report may be limited if it is unable to obtain additional information from you if required.

If you believe that you may have breached the Code or any policy of the Company that applies to you, or if you have observed a breach of the same by another employee, or a serious weakness or deficiency in the Company's policies, procedures or controls which might enable breaches to occur or to go undetected, you have a responsibility to report this immediately.

Genuine concerns, raised in good faith, will be investigated fully. As a rule and as outlined in the Company's "Fraud and Other Wrongdoing Policy", the Company will not permit any reprisal, retaliation or disciplinary action to be taken against anyone for raising a concern in good faith. It is a breach of this Code to make a mischievous or malicious report.

6 Code Policies, Standards and Procedures

Each compliance requirement in the Code is backed up by compliance standards and procedures that facilitate the effective operation of the Code. The standards ensure prompt and consistent action against violations of the Code. The elements of the Code themselves are to be found in Company policies or corporate governance guidelines that support the Company's internal control framework. Some related policies are listed below:

- Insider Trading Policy
- Electronic Mail and Internet Security Policy
- Password Policy
- Fraud & Other Wrongdoing Policy
- Anti-Money Laundering and associated Policies
- Information Security Policy
- HR Policies

7 Code Waivers

Exceptions to the Code will not be granted where the principle or spirit of the code is compromised. Waivers will be considered in those very exceptional situations where a provision may have inadvertently cast too wide a net.

All requests for waivers are to be submitted to the Group Compliance Officer, who will ensure the request is supported by sufficient reasoning, evidence and facts upon which to base a rational decision. The Group Compliance Officer will arrive at a judgment as to whether the waiver will be granted and submit his/her recommendation to the President and CEO in the case of non-executive employees and to the Chairman of the Corporate Governance Committee if executives and directors request the waiver. The Committee will make its decision and present its recommendation to the full board for approval.

The Group Compliance Officer compiles and presents a report quarterly to the Audit Committee of all waivers granted in the Company and amendments to the Code. This report forms the basis for shareholder disclosure.

8 Internal Communications Procedures

If you are unsure of the legal, ethical or reputational implications of a particular situation, or would like further guidance related to a matter referenced in this Code, you should consult first with senior officers within your business area and if necessary, go next to the Company Compliance Officer. Directors should consult the Chairman of the Board or the Chairman of the Corporate Governance Committee.

If you believe there is a conflict between this Code, any Business Practices and Procedures, and any legal or regulatory requirements that apply to you in your position with the Company, you should contact the Company Compliance Officer.

9 Conflict between the Code and Local Laws

The Code and the policies of the Company have been written to foremost promote compliance with the law. Should compliance with the Code or any policy of the Company bring you into conflict with applicable law in any jurisdiction where the Company operates, you must obey the law first. Thereafter, immediately notify your supervisor or manager of the conflict so that the conflict may be promptly resolved. If you have questions or concerns about practices or policies that might violate the Code, bring them to the attention of your superior officer immediately.

10 Annual Acknowledgement

After your initial orientation and each year subsequently, you will be asked to acknowledge that you have read the Code, that you understand your obligations under it, and that you agree to comply with it. At the same time, you will also be asked to confirm that you have complied with the Code during the prior year, that you have reported any breaches of the Code as required, or if necessary, take the opportunity to report any current breaches. The forms, Internal Disclosure Certificate and the Annual Declaration of Income, Assets and Liabilities, shown as Appendix A are to be used for this purpose. However, in no event will compliance with this Code create any right to continued employment or appointment**.**

11 Availability of Code

This Code along with some other related policy documents is available on the Company's website at www.sagicor.com as well as on the AlertLine website at www.sagicor.alertline.com.

Published August 2008.

Document History & Version Control Table			
Version	**Action**	**Approval Authority**	**Action Date**
1.00	**Original Document published**	**SFC**	**August 2008**
1.01	**The section 1.2 Disclosure was added along with the Annual Declaration of Income, Assets & Liabilities form to Appendix A. Amendments were made in keeping with enhanced Know Your Employee (KYE) regulatory requirements.**	**SGJ Corporate Governance & Ethics Committee**	**June 2016**

APPENDIX A

SAGICOR GROUP JAMAICA LIMITED

ANNUAL DECLARATION OF INCOME, ASSETS & LIABILITIES

DECLARATION PERIOD: _____ TO _____

SECTION A:
PARTICULARS OF TEAM MEMBER

FULL NAME: | | | |
FIRST MIDDLE LAST

DEPARTMENT: | | UNIT: | |

TITLE: | | TEAM MEMBER NUMBER: | |

TRN: | |

PLACE OF EMPLOYMENT: ☐ BANK ☐ INVESTMENT ☐ LIFE ☐ EBA LTD.

NUMBER OF YEARS EMPLOYED: | | (at SAGICOR)

| | (other institution(s))

SECTION B:
DECLARATION OF ASSETS

Tick (✓) the value category under which your assets would fall. (Please include property owned by the team member and held in another person's name or jointly held with another person). Please use current market value.

ASSETS	**Under $1M**	**Over $1M – Under $2M**	**Over $2M- Under $5M**	**Over $5M- Under $10M**	**Over $10M**	**N/A**
1. Savings/Deposit Account						
2. Real Estate (House, Land etc.)						
3. Furniture						
4. Investments (stocks, shares & other investments)						
5. Life Insurance Cash Value						
6. Other Assets						

Indicate Type(s): _____

_____

_____

	Under $1M	Over $1M – Under $2M	Over $2M- Under $5M	Over $5M- Under $10M	Over $10M	N/A
7. Income from Other Sources						

Indicate Source(s): _____

_____

8. Assets bought during the year						

Indicate Type(s): _____

_____

9. Assets sold during the year						

Indicate Type(s): _____

_____

10. Motor Vehicle						

Indicate Make & Model: _____

Year: _____

Purchase Price: _____

SECTION C:
DECLARATION OF CURRENT LIABILITIES

Tick the value category under which your liabilities would fall.

LIABILITIES	Up to $1M	Over $1M - $2M	Over $2M- $5M	Over $5M- $10M	Over $10M	N/A
1. Mortgage Loan						

Name & Address of Mortgage Company: _____

_____

2. Motor Vehicle Loan						
3. Furniture Loan						
4. Current Account						
5. Overdraft (Limit)						
6. Other Liabilities						

Indicate Types (s): _____

_____

I certify that the information given above is to the best of my knowledge true and accurate and that I understand that the said information will form part of my employment records.

Respondent's Signature _____

Date _____

INTERNAL DISCLOSURE CERTIFICATE

		Yes	**No**
1	I have read the Sagicor Code of Business Conduct and Ethics ("Code")		
2.	I have been given an orientation on the key aspects of the Code.		
3	I fully understand my ethical duties as explained in the Code.		
4.	I am currently, or during the past year have been, involved in the following outside activities		
	a) Second jobs or other commercial activities (officers and employees only)		
	b) Outside Paid Directorship (all)		
	If you answered "Yes" to # 4, please provide details here.		
5.	I am at this time in full compliance with the Code		
	If you answered "No" to the above, please list below your situations of non-compliance:		
6.	I have disclosed my (potential) conflict situations above.		
	If you answered "No", explain below		
7.	I commit to promptly report any non-compliance with the Code, whether my own or that of any other director, officer or employee not disclosed.		
8.	I have fully and accurately completed the Declaration of Income, Assets and Liabilities form along with this Disclosure Certificate		

Please submit this Certificate to your reporting Officer (Officer and employees) or to the Corporate Governance Committee (directors) for onward transmission to the Group Compliance Officer.

Respondent's Signature

Reporting Officer's Signature

Respondent's Name

Reporting Officer's Name

Date

Date

Revised July 2015

APPENDIX B

USING ALERTLINE

Computer:

Step 1: Connect to the Internet from a computer outside of work

Step 2: Type **www.alertline.com** into the address bar and hit "Enter"

Step 3: Search for your company's name

Step 4: Enter your company's name into the box provided. To eliminate the first 4 steps you may go directly to **www.sagicor.alertline.com**

Step 5: Select your method of anonymous communication and enter the desired information.

Note: You need not provide your name or any other form of identifying data.

Telephone:

Step 1: Dial your country's access code selected from the list below.

Step 2: When prompted dial **YOUR TOLL FREE ALERTLINE ACCESS NUMBER 1(888)307-5991** to speak anonymously with a live hotline operator.

Step 3: Provide the operator with the desired information

Access Codes:

Anguilla: 1-800-225-5288

Aruba: 001-800-872-2881

Antigua & Barbuda: 1-800-225-5288

Bahamas: 1-800-872-2881

Barbados: 1-800-225-5288

Belize: 811

Cayman Islands: 1-800-225-5288

Dominica: 1-800-225-5288

Grenada: 1-800-225-5288

Jamaica: 1-800-872-2881

Netherland Antilles (Curaçao and St. Maarten): 001-800-872-2881

Panama: 800-0109

St. Christopher & Nevis: 1-800-225-5288

St. Lucia: 1-800-225-5288

St. Vincent & the Grenadines: 1-800-225-5288

Trinidad & Tobago: 1-800-872-2881

United States: no access code necessary dial toll free number directly.



STOCKBROKERAGE POLICY

Table of Contents

1 INTRODUCTION 5
2 OBJECTIVE 5
3 RELATED ACT AND EXTERNAL GUIDELINES 5
4 GLOSSARY OF TERMS 5
5 MANAGEMENT & MAINTENANCE OF MANUAL 6
6 DEALER REPRESENTATIVES 6
7 SEGREGATION OF DUTIES 7
8 TRADERS' CONDUCT 7
9 PERSONAL TRADING & TRADING FOR CONNECTED PARTIES 8
10 INSIDER TRADING AND PROTECTION OF INFORMATION 8
11 SHORT SELLING 9
12 CLIENT DUE DILIGENCE AND COUNTER PARTY CREDIT LIMITS 9
13 STOP LOSS AND OPEN POSITION LIMITS 10
14 TRADE CONFIRMATION AND SETTLEMENT 10
15 TRANSACTION PRIORITY 11
16 OTHER BROKER EMPLOYEES 11
17 FAIR DEALING 12
17.1 Dissemination of Information 12
17.2 Discrimination 12
17.3 First-In – First-Out 12
17.4 Allocation Policy 12
17.5 Private Placements and Initial Public Offerings (IPO) 13
18 BLACK OUT PERIODS 13
18.1 Cancel Orders during Blackout 14
18.2 Exceptions to Blackouts 14
19 RESTRICTED TRANSACTIONS 14
20 SANCTIONS 15
21 PROPRIETARY TRADING 15
22 COMMISSIONS AND FEES 15
22.1 Other Stockbrokerage Fees 15
22.2 Changes to Fees and Commissions 15
23 APPENDIX 16

23.1 Examples of Material Information 16

23.2 Approval Request for External Brokerage Account 16

23.3 T+2 APPROVAL LIMITS 17

23.4 Approval for T+2 Settlement Form 18

Revision History

Policy ID: **POL-INV-STOCKBROKERAGE07-2021**	Title: **Stockbrokerage Trading Policy**	Date **2/7/2021**
Revision **2021**	Prepared By: **Susan Dear, Independent Consultant**	Date Prepared **March 2021**
	Reviewed By Treasury & Trading: **Roger McKenzie, AVP, Treasury & Trading**	Date Reviewed **March 2021**
	Reviewed By Enterprise Risk Management and Group Compliance: **Caren Scott-Dixon – Head of ERM & Group Compliance**	Date Reviewed **March 2021**
	Reviewed By Group Legal: **Jassetta Jones - AVP, Group Legal**	Date Reviewed **March 2021**
	Reviewed By: **Tara Nunes, Chief Executive Officer**	Date Reviewed **June 2021**
Effective Date:	Approved by: **Sagicor Investments Board of Directors**	Date Approved **July 2, 2021**

1 INTRODUCTION

This policy exists to provide the guidance needed to ensure that related equity trading activities performed by Sagicor Investments Jamaica Ltd. (SIJL) and its subsidiaries, are being conducted in accordance with applicable laws, regulations and industry best practices. This policy should be read in tandem with the SIJL Investment Policy approved by the Board governing all asset classes.

2 OBJECTIVE

- To provide guidance to team members involved in the trading of clients' securities as well as trading on behalf of SIJL and its subsidiaries.
- To ensure documented controls are in place intended to reduce financial legal and regulatory risk exposures.
- To provide guidance to team members involved with personal trading; self-dealing in the trading of shares and conflict of interest.

3 RELATED ACT AND EXTERNAL GUIDELINES

This section lists related documents needed to provide the reader with additional context or information in order to have a better understanding.

There may be changes in the respective policies listed and therefore users are reminded to review the related documents to identify any updates.

- The Securities Act
- The Jamaica Central Securities Depository Rules
- The Jamaica Stock Exchange Rules Book
- SIJL Investment Policy

4 GLOSSARY OF TERMS

Terms	Definitions
Access Person	Person who has access to nonpublic information regarding clients' purchase or sale of securities, is involved in making securities recommendations to clients or who has access to such recommendations that are nonpublic
Connected Parties/Persons	Persons deemed to be connected with a director/senior manager (VP and above): • The director's/senior manager's husband or wife.

Terms	Definitions
	• The director's/senior manager's minor children (these include step-children and adopted children) and dependents, and their spouses. • The director's/senior manager's partners. • Bodies corporate of which the director/senior manager and/or persons connected with him/her together have control.
Control	The holding of shares which carry 50% or more of the voting rights in a corporation.
ERMGC	Enterprise Risk Management & Group Compliance
FSC	Financial Services Commission
GTAM	Group Treasury Asset Management
IRMC	Investment and Risk Management Committee
JCSD	Jamaica Central Securities Depository
JSE	Jamaica Stock Exchange
False Trading	Acts intended or likely to create a false or misleading impression of active trading in securities on a securities exchange
Market/Price rigging	An illegal action that occurs when parties conspire to fix or inflate prices to achieve higher profits at the expense of the consumer
Market manipulation	the act of artificially inflating or deflating the price of a security or otherwise influencing the behavior of the market for personal gain
Front-running	Trading stock or any other financial asset by a broker who has inside knowledge of a future transaction that is about to affect its price substantially

5 MANAGEMENT & MAINTENANCE OF MANUAL

The policy should be reviewed at least annually by SIJ's Management Team with advice and counsel provided by the Enterprise Risk Management & Group Compliance (ERMGC) Unit, re proposed amendments. Approval of the Stockbrokerage Trading Policy is the responsibility of the Board of SIJL and relevant sub-committees.

The ERMGC Unit will monitor and evaluate compliance with the policy on a regular and ongoing basis along with the Internal Audit Unit which will conduct independent reviews/compliance during their audit process.

6 DEALER REPRESENTATIVES

The Securities Act requires all Dealer's Representatives and Investment Advisors to be licensed by the Financial Services Commission (FSC) and the Jamaica Stock Exchange (JSE). Only licensed Dealer's Representatives are therefore authorized to engage in trading activities on behalf of the company; it is

the responsibility of the Head of Treasury and Trading to ensure that all traders under his/her supervision are duly licensed. Where an application for a Dealer's Representative License is to be made, the Head of Treasury and Trading should ensure the relevant forms are completed and submitted with supporting documentation to the Financial Services Commission.

All Traders must read and adopt the standards of conduct set out in the JSE Main Market Rules which are incorporated by reference into this policy. The standards to be complied with include but is not limited to the following:

- Observing and promoting a high standard of professional and ethical conduct
- Complying with fiduciary principles in dealings with clients
- Full disclosure of personal investment, activities and decisions to clients and company
- Fair Dealing with clients
- Not engaging in False Trading, Market Rigging and Manipulation or trading ahead of customer orders
- Avoiding and disclosing all conflicts of interest
- Observing confidentiality and protection of material non-public information
- Prohibition on insider trading

All SIJL employees are required to review the Stockbrokerage Policy annually and attest to same. Group HR shall maintain these records.

7 SEGREGATION OF DUTIES

The maker/checker process for trade transactions is an important segregation of duties mechanism that ensures that an individual is not given complete authority and control over an entire process. In addition to the Investment Advisor and Trader the Equity Order Form is to be signed by both the officer who entered the transaction and the officer who approved the transaction.

8 TRADERS' CONDUCT

The Securities (Conduct of Business) Regulations outlines in the Standards of Professional Conduct that all licensees must establish the continuous monitoring and review of trading activities of Traders and registered representatives in order to mitigate the risk of unethical behaviour such as front-running.

Periodically, review of transactions processed by personnel involved in the execution of trades on behalf of the company and its clients will be coordinated by Internal Audit and Compliance. Annual declarations are also made by team members to the Human Resource Department on their financial holding/assets.

Traders are prohibited from engaging in Front-Running activities either on their own behalf or on behalf of someone connected to them. Front-Running occurs where a Trader trades an actively traded security based on information from analysts before his or her clients have been given the information and have

an opportunity to act on it. Front-Running also occurs where a Trader takes a position in a security just before his firm plans to trade a large block of that security.

9 PERSONAL TRADING & TRADING FOR CONNECTED PARTIES

As per the Securities Act, Compliance must monitor to ensure that the personal investment activities of all officers and registered representatives of SIJL are disclosed. To facilitate full disclosure, team members are therefore encouraged to maintain their stock brokerage accounts with SIJL.

Team members who opt not to maintain their Brokerage accounts with SIJL must obtain written approval (see Appendix for Approval Request Form) from the Head of Human Resources and the CEO. Approval will only be given where another brokerage offers products or services which are not available with SIJL. In the event approval is given, it is the responsibility of the team member to submit statements or transaction confirmations evidencing all stock holdings or transactions to Group HR within one (1) week of the acquisition or transaction.

All Team members must also complete the Declaration of Holdings which is sent via a link annually from Group HR in respect of their own holdings and those of any closely connected parties. If no transactions take place the Declaration of Holdings should still be submitted at the beginning of each year. Group HR shall maintain these records.

Traders who maintain brokerage accounts with SIJL should not process or handle their own trades. These trades must be approved by a Senior Manager before execution.

Related/Connected party trades are to be submitted by the Trader to the Corporate Secretary of the respective listed entities within the Sagicor Group for filing with the Regulatory & Market Oversight Division (RMOD) of the JSE on the day the trades are executed. These trades are also to be reported to the Board of Directors of the relevant listed entities within the Sagicor Group at scheduled meetings.

10 INSIDER TRADING AND PROTECTION OF INFORMATION

Section 51 of the Securities Act and Section 9(1b) of the Securities (Conduct of Business) Regulations outlaws Insider Trading. Insider Trading occurs where an insider or a related party trades based on material non-public information obtained during the performance of the insider's duties or otherwise misappropriated. It is the responsibility of all staff members, (particularly those members of the Capital Markets, Research, Credit and Financial Control Units who more frequently come into contact with material non-public information) to maintain and protect the strict confidentiality of such information (See Appendices for examples of material information).

Material nonpublic information must not be disclosed to anyone, except the persons within the Company or third party agents of the Company (such as outside legal counsel) whose positions require them to

know it, until such information has been publicly released by the Company. Improper disclosure or handling of material non-public information will result in disciplinary action including dismissal.

Access to the trading room, Capital Markets, Research Unit, Financial Control and other areas where material non-public information is prepared, circulated and discussed should be restricted to persons who should have access to such areas to perform their functions. Where this prohibition is not entirely possible, documentation containing material non-public information must be kept strictly confidential and access to it restricted to those who need access to perform their functions.

11 SHORT SELLING

The Securities Act restricts the short selling of securities in certain instances. Short Selling occurs where a party sells securities which he does not possess; this creates a negative position in the security. Short Selling will usually occur where securities are borrowed from one counterparty, pursuant to an agreement, and sold to another. The Securities Act prohibits short selling where the seller does not have an unconditional right to vest the security in the buyer, in other words, there is no agreement with the owner of the security and SIJL has no legal or beneficial title. The following transactions are therefore prohibited:

- Borrowing Securities from custodial or safekeeping clients for trading where the client has not executed an agreement to lend the security;
- Trading securities being used to back reverse repurchase agreements where the client has not executed SAGICOR INVESTMENTS' General Investment Terms and Conditions;

It is the responsibility of the designated GTAM Officer to ensure trading does not take place where SIJL does not have an unconditional title to the security.

There should therefore be no commingling of client securities (custodial) and those used for trading. Separate up-to-date registers should be maintained by the designated responsible Stockbrokerage BSU officer and GTAM officer respectively in compliance with the Securities Act Regulations.

12 CLIENT DUE DILIGENCE AND COUNTER PARTY CREDIT LIMITS

Part III Section 8(2a) of the Securities (Conduct of Business) Regulations requires dealers to make enquiries to establish the identity, reputation and where applicable, the credit-worthiness of each client. As such, SIJL client due diligence policies as set out in the Sagicor Group Anti-Money Laundering Policy are incorporated by reference into this policy. It is the responsibility of the Client Services representative (i.e. Wealth Advisor/CRO) to ensure that sufficient information has been collected to establish the client's identity, reputation and credit worthiness. If sufficient client due diligence documentation has not been collected, representatives must not negotiate trades with the client.

Client due diligence practices which include an assessment of the client's credit worthiness, are critical to managing counterparty risk. Counterparty Risk is the risk that another party to an agreement will default resulting in a loss to SIJL. Refer to the Sagicor Investment Policy detailing the setting of counterparty credits which must be complied with.

13 STOP LOSS AND OPEN POSITION LIMITS

SIJL has established position and stop loss limits in its Investment Policy to manage market risk exposures.

It is the responsibility of the ERMGC unit to monitor the total open equity position and the prices of all "quoted" equity securities and report on any breach in stop loss and/or position limits. However, once a decision has been made to trade, it is the trader's responsibility at first instant, to review the blotter (summary sheet) to determine whether the implemented limits (including position and stop loss) would be breached and to ensure that it is not.

In the event a trade has been concluded which would result in a limit breach, SIJL is required to provide an action and a timeline for remedying the breach which may include offloading the position. SIJL will be required to request approval from the IRMC in this regard.

14 TRADE CONFIRMATION AND SETTLEMENT

All trades executed on the floor of the JSE will settle through the JCSD on T+2. This means that on T+2, SIJL will either pay or receive net settlement amounts to/from the JCSD. SIJL operates a Settlement Account with the Settlement Bank (BOJ) and a JCSD Participant Account. These accounts are used solely for effecting the actual payment of the net settlement obligations of itself and the JCSD. Payment to the JCSD is made via RTGS through irrevocable arrangements with SIJL.

Where purchases exceed the sales of shares on a specific trade date, Brokers are required to pay the net settlement amount to JCSD. Similarly, where sales exceed purchases on a specific trade date, JCSD will transfer funds to credit the Broker's designated Bank of Jamaica (BOJ) account. Stockbrokerage Operations will receipt all funds for settlement of client trades to the clients' respective settlement accounts.

The Stockbrokerage Operations will compile the deposit for the bank and if there is a shortfall to cover any outstanding balance, they are to notify the Fixed Income Trader to fund Stockbrokerage bank account.

The Trading Manager is authorized to sell the securities and credit the proceeds to the Broker Account (after deducting all charges) for clients that having outstanding balances for longer than the allotted settlement period. An interest charge may also be levied; the client must be advised of these actions.

The CSR is to ensure that funds are available in the client's settlement or investment account before the equity order is placed with the Trader. Based on the clients' relationship history, net worth and knowledge of the client, a client may be approved to provide settlement on T+2 either on a one-off basis or through a pre-approval process. Approval must be obtained from two senior managers (AVP and above) using the Approval for T+2 Settlement form (in the case of pre-approval) or via email for one-off trades.
See appendix 23.3

A list of pre-approved clients for T+2 settlement is to be maintained and updated by SIJL Stockbrokerage Business Support Unit. This list should be reviewed annually by the BSU in conjunction with the Head of Wealth and Client Services.

15 TRANSACTION PRIORITY

While orders should be processed and executed on a first-in, first-out basis, the Securities Act requires priority to be given to client's transactions. Traders must therefore not enter into proprietary transactions for the purchase and sale of equities on behalf of SIJL or a connected party where a client has already given a buy or sell instruction in the same shares that remains unexecuted.

Priority may however be given to SIJL orders or those of a connected party where the client has requested the purchase or sale to take place under specified conditions; for example at a given price and those conditions have not yet been satisfied or where client orders are received after those of SIJL or connected parties. Connected parties include Senior Managers and Directors as well as general staff and affiliated companies.

16 OTHER BROKER EMPLOYEES

In accordance with Rule 223 of the Jamaica Stock Exchange no account should be opened for or business transacted where the employee of another member of the Stock Exchange has a direct or indirect interest in the account or transaction without prior approval of the employer (stock exchange member).

It is the responsibility of the contact person, (whether Trader or Client Services Representative), to determine at the time of opening the account or initiating the transaction, whether the prospective client is an employee of another member of the Stock Exchange. No member/dealer is to knowingly take or carry any account or make any transaction in which any employee of another member/dealer has an interest, either direct or indirect, without the written consent of such other member/dealer. All equity transactions with clients who are employees of Stock Exchange members should be reported to the ERMGC unit.

17 FAIR DEALING

SIJL insists upon the adoption of Fair Dealing Principles in the provision of professional services to its clients. As such, traders and investment services personnel are required to deal fairly, equally and objectively with all clients as outlined in the 'Code of Conduct'. No client or group of clients should be systematically disadvantaged by the allocation of investment advice or opportunities. In adopting Fair Dealing Principles, the following policies must be followed.

17.1 Dissemination of Information

While it is impossible to disseminate information, advice or recommendations about investment opportunities to all clients equally and at the same time, it is SIJL's policy that dissemination should be as equitable as possible, in this regard traders and investment services personnel should: -

- Maintain and continually update their client lists so they are able to identify different categories of clients by the suitability of differing investment opportunities to them. This will aid the fast dissemination of information which may be of particular importance to a particular group.
- Ensure that whatever the means of notifying clients, they strive to ensure that as many are notified in the smallest timeframe as possible so all have an equal opportunity to assess and act on the recommendation or advice. For regular bulletins with a narrow window of opportunity they should strive to maintain e-mail addresses for as many clients as possible since this allows for quick simultaneous notification even though receipt may not occur simultaneously.

17.2 Discrimination

All clients should be treated fairly and advised if there are superior services for which they may qualify. When taking investment actions or disseminating information, traders and investment advisors should strive to ensure that clients within the same service group are not discriminated against and that one client is not favored over others especially on the basis of higher potential commissions and fees.

17.3 First-In – First-Out

Where securities are being traded, client orders are to be processed and filled on a first in first out basis. This means that orders received first in time should be processed before later orders that have the same execution price. All client orders must be date and time stamped on receipt to record the time of the order and to ensure it is processed in the order in which it is received unless the client has set special conditions such as price and quantity requirements which preclude the order being filled until those conditions are met.

17.4 Allocation Policy

- Where SIJL executes block orders for clients participating in block trades and the order is only partially filled, the partially executed order will be allocated among the participating client accounts pro-rata on the basis of each client's share of the total order.

- All clients participating in a block order or Private Placement must be given the same execution price and charged the same proportionate commission.
- The method of allocation and setting the execution price should be disclosed to the client upon request.
- Where SIJL participates in a block order for its proprietary positions and the order is only partially filled, SIJL will make no allocation to itself if the partially filled block order is insufficient to satisfy the order of clients who also participated. SIJL will only allocate to itself if the client's orders have been fully satisfied.
- Spinning occurs where securities are allocated to an executive officer or director of a company on condition that he directs the company's future investment business to the spinner. This practice is prohibited.

17.5 Private Placements and Initial Public Offerings (IPO)

Initial public offerings occur when a company first sells its shares to the public as a means of raising capital. A private placement occurs where securities are sold directly to institutional investors and/or an Accredited Investors as a means of raising capital, and such securities may then be resold. IPO's and Private Placements are frequently "hot offerings" with the demand for these securities exceeding the supply. Where SIJL participates in an IPO or a private placement of securities for resale to its clients, Team Members or connected parties, the aforementioned allocation policy must be used to determine how orders are to be satisfied.

18 BLACK OUT PERIODS

A "blackout period" refers to a period during which trading in designated securities is prohibited regardless of whether those securities are held with SIJL. It is the responsibility of the Company Secretary to advise of the designated "blackout periods" during which team members should not trade in equities or other securities so specified.

A blackout period will begin Fifteen (15) days after the end of each quarter and will remain in effect until the quarterly financial returns have been made public (no later than 45 days after the end of the quarter). For the final quarter, the blackout period will begin at the end of the quarter and last until the annual financial results are published in 60 days (28th February).

Quarter or Year End	Release of Accounts	Black Out Periods	Trading Periods	Length of Trading Period
Mar 31 - Q	May 15	Apr 15 - May 15	Apr 1 - Apr 14	2 weeks
Jun 30 - Q	Aug 15	Jul 15 - Aug 15	May 16 - Jul 14	8 weeks
Sep 30 - Q	Nov 15	Oct 15 - Nov 15	Aug 16 - Oct 14	8 weeks

Dec 31 - Y/E audit	End of Feb	Jan 1 – Feb 28 or until financials are finalized	Nov 16 – Dec 31	

The following occasional blackout periods are also imposed: -

- Regarding SJ shares, where a company announcement of material non-public information is made, and the period beginning on the day of the announcement and ending at the end of the business day after the day of the public announcement.
- Regarding instances where SIJL is conducting analysis on the condition of an issuer and/or has material non-public information about the issuer, the beginning of the analysis period and ending at the end of the business day after the day of the announcement of the results of the analysis.

Notwithstanding the foregoing, trading will not be allowed at any time whilst having knowledge of any material non-public information regarding the company, which could impact the price of the company's shares. Access persons are required to write and seek acknowledgement from the Chairman on trades and the Company Secretary will maintain records pursuant to those trades.

18.1 Cancel Orders during Blackout

Orders whether placed with another Dealer or Brokerage (with permission) or with SIJL for the purchase or sale of Sagicor Group Jamaica shares must be satisfied before the beginning of a blackout period. Orders or transactions which are not completed by the start of a blackout period must be terminated immediately; failure to terminate the order will be regarded as an infringement of the blackout restrictions and may incur disciplinary action.

18.2 Exceptions to Blackouts

Rights and Bonus Issues are not affected by the aforementioned blackout restrictions. Access Persons and team members in general are free to take up these Issues whenever they are offered.

19 RESTRICTED TRANSACTIONS

Directors, Officers, Employees, and connected parties may not trade in options, warrants, puts and calls or similar instruments on Sagicor Group Jamaica (SJ) shares. However, anyone may exercise options granted to them by Sagicor Group and sell shares acquired through option exercises, subject to the restrictions discussed in this Policy and other applicable Company policies.

20 SANCTIONS

Failure to comply with the provisions of this policy will result in disciplinary action up to and including dismissal. Team Members and "Access Persons" should also note that some of the requirements and prohibitions under this policy are in accordance with the provisions of the Securities Act and the Securities Act Regulations, non-compliance may also attract criminal liability.

21 PROPRIETARY TRADING

Proprietary trading also known as "prop trading," refers to when SIJL invests directly in the market for the company's gain rather than earnings only from commission made by trades on behalf of clients. Proprietary trading may involve the trading of stocks, bonds, commodities, currencies or other instruments.

As mentioned in Section 10 Transaction Priority, Traders must not enter into proprietary transactions for the purchase and sale of equities on behalf of SIJL or a connected party where a client has already given a buy or sell instruction in the same shares that remains unexecuted. Trading levels that trader execute is governed by the Sagicor Investment Policy which is reviewed annually.

Where SIJL participates in a block order for its proprietary positions and the order is only partially filled, SIJL will make no allocation to itself if the partially filled block order is insufficient to satisfy the order of clients who also participated. SIJL will only allocate to itself if the client's orders have been fully satisfied.

22 COMMISSIONS AND FEES

Fees and commission are charged for trades executed on behalf of clients. Fees charged on trades executed include: Trade Fees, GCT on Trade Fees, CESS, and GCT on CESS. Commission charged is in the form of a Broker commission. This attracts a GCT on commission. Commissions are charged based on the client's commission category assigned. Commission/Fees are to be disclosed to clients and transparency maintained re changes to these charges.

22.1 Other Stockbrokerage Fees

Fees are charged for other Stockbrokerage services such as Lodgment and Withdrawal of Certificates, Pledging of Shares, as well as Inter and Intra Member Movement of Shares. All fees and GCT thereon must be collected prior to execution of the client's request. Stockbrokerage operations must receipt fees received from clients for these services. Fees collected are to be paid to the JCSD and JSE at the end of each month.

22.2 Changes to Fees and Commissions

Fees and commission charged are subject to change based on changes made by the JSE and the JCSD, changes to General Consumption Tax percentage (GCT), and the commission structure of the Broker. Changes to fees are to be disclosed to clients and transparency maintained re changes to same.

Changes required to Stockbrokerage fees and commissions may be inputted and authorized by Stockbrokerage Operations upon receipt of the necessary approval to do so.

Requests for changes to fees must be received by the Stockbrokerage Operations Unit from the CEO electronically or in writing prior to being implemented in the T24 system.

Requests for changes to commission charges, including team members' rates must be received by the Stockbrokerage Operations Unit and approved by any 2 of the following: CEO, Vice President, AVP Treasury, or Trading Manager electronically or in writing prior to being implemented in the T24 system.

23 APPENDIX

23.1 Examples of Material Information

- Proposed acquisitions or sale
- Financial results
- Senior Management Changes
- Events that could result in re-stating financial information
- Gain or loss of substantial business contract/bid
- Dividend policy changes or other dividend news
- News of a pending or proposed merger
- Impending bankruptcy or liquidity Issues
- New equity or debt offerings, significant new product news
- Significant litigation exposure, pending or actual regulatory action
- Projections of earnings or losses
- Significant product defects, modifications or recalls

23.2 Approval Request for External Brokerage Account

Date	Name of Team Member
Position of Team Member	

In accordance with the provisions of the Stockbrokerage Trading Policy, I hereby request permission to open a brokerage account with another member of the Jamaica Stock Exchange. My request is based on the provision of the following services which are not offered by SIJL -

Details of Brokerage

Name of Brokerage

Address of Brokerage

If my request is approved, I give my undertaking to provide transaction confirmations in the event I execute any trade through this account or if no trades are executed in a calendar year, to provide a statement of my holdings in the account.

Signature of Team Member

Date

FOR OFFICIAL USE

Your request for permission to open an account with another broker has been: -

☐ **Approved**

☐ **Declined**

Authorized Officer

Approval Date

This section should only be completed at the specific request of the Compliance Officer

23.3 T+2 APPROVAL LIMITS

Sagicor Investments Jamaica Limited
Stockbrokerage Pre-approved T+2 Trading Limits
Jun-21

AUM or Net Worth J$ (or US$ Equiv.)	Approved Trading Limit J$ (or US$ Equiv.)	Approval Level
<25M	up to J$10M	1 AVP or above
25M-50M	up to J$25M	2 AVP or above
>50M	up to J$50M	1 AVP and CEO

23.4 Approval for T+2 Settlement Form

Sagicor Investments

Approval for T+2 Settlement
Form ATS-062021

Request for client to settle purchase of equities on T+2.

Forward form to senior management (AVP and above) for approval. Business support will add to existing list of approved clients and circulate to Traders and Wealth Advisors.

Client Information
Client Name (for individuals only Primary applicant name required):
Existing SIJL Client: ☐ Yes ☐ No If yes state: • Client Information No. Client Brokerage Settlement a/c No.
Qualifications for approval: ☐ Net Worth – state amount ☐ History & Relationship with SIJL. State # of years : ☐ Assets under management with SIJL ☐ Well known established Client Provide further information below that could contribute to approval. Approved T+2 Trading Limit:

AUM or Net Worth J$ (or US$ Equiv.)	Approved Trading Limit J$ (or US$ Equiv.)
☐ <25M	up to J$10M
☐ 25M-50M	up to J$25M
☐ >50M	up to J$50M

APPROVAL		
Requestor:	**Signature**	**Date (dd/mm/yy)**
Approved by:	**Signature ☐ email approval**	**Date (dd/mm/yy)**
Approved By:	**Signature ☐ email approval**	**Date (dd/mm/yy)**

Sagicor

Wise Financial Thinking for Life

Sagicor Group Jamaica Ltd.

Data Classification Policy

Version 1.0

October 2024

Data Classification Policy

TABLE OF CONTENTS

1 INTRODUCTION: 4

2 ROLES AND RESPONSIBILITIES: 5-9

3 TERMS AND DEFINITIONS 9

4 DATA CLASSIFICATION PRINCIPLES 9-10

6 RISK LEVELS 11

5 DATA CLASSIFICATIONS 12-15

7 POLICY DETAILS 16

8 REVIEW OF POLICIES 17

9 EXCEPTIONS 17

10 EFFECTIVENESS CRITERIA 17

11 POLICY COMPLIANCE 18

12 APPENDIX 18

Policy ID **POL_DAD_DCP_102024**	Title: **Data Classification Policy**	Version **1.0**
Classification	Sagicor Internal	Date Published
Prepared By	Renesha Robinson *Business Research Analyst*	Date Prepared **05/01/2024**
Reviewed By	Data Governance Committee (DGC) Group Internal Auditing Group Legal IT & Data Security Enterprise Risk Management & Group Compliance	Date Reviewed **08/14/2024**
Committee Approval	SGJ IT Steering Committee	Date Approved **04/25/2025**
Committee Approval	SGJ and SLJ Corporate Governance & Ethics Review Committee	Date Approved **02/28/2025**
Board approval	SGJ Board	Date Approved **07/31/2025**
Policy Owner	Opal Donaldson Vice President – Data Privacy & Analytics	

1 INTRODUCTION

1.1 What is data classification?

1.1.1 Data classification is fundamental to any data security and privacy program. It provides visibility into the data categories, identifies the value, confidentiality and sensitivity of the data to the organization (Sagicor) and helps organizations (Sagicor) determine which controls should be in place.[1]

1.2 Why must data be classified?

1.2.1 Without the appropriate levels of classification administered, sensitive and personal data becomes exposed and vulnerable to cybersecurity threats and other related security risks/hazards which can result in data breaches and the organization potentially being fined. Additionally, this ensures as an organization we are in keeping with data protection regulations and standards specific to the operating region.

1.3 PURPOSE

1.3.1 As an organization, Sagicor Group Jamaica (SGJ) has a responsibility to ensure that the appropriate level of protection is identified and applied to prevent the loss or damage to data produced, shared, and used by or in the care of the company.

All employees of Sagicor have a responsibility to ensure that data owned by the company or entrusted to the company by clients is protected from unauthorized access or disclosure. This document serves as a reference guide for classifying Sagicor's data.

[1] See Bales, A., Henein, N., & Willemsen, B. (2024). Toolkit: Classification and Handling of Sensitive Data. GARTNER. https://www.gartner.com/document/5095831?ref=solrAll&refval=420238114&

1.4 SCOPE

1.4.1 This policy applies to ***All*** who require access, either from internal or external locations to any of Sagicor's data assets. This includes:

- Sagicor team members
- Temporary employees
- Contractors
- Consultants
- Financial Advisors/Agents
- Volunteers, and individuals affiliated with third parties

All company data or information created, processed, or used in support of Sagicor's operations, regardless of the form, format, division, or subsidiary is covered by this policy unless otherwise exempted by senior management in writing (See Section 9, Exceptions).

1.5 POLICY STATEMENT

1.5.1 It is the policy of Sagicor Group Jamaica to ensure that all data regardless of its format collected, stored and used by or in the care of the organization is classified and handled according to classifications and risk levels outlined in this document. This policy shall be defined in line with the applicable regulatory, legal and contractual obligations as well as business requirements and industry best practices.

2 ROLES AND RESPONSIBILITIES

2.1 The following key stakeholders have a role to play in ensuring that the data is managed and used in accordance with the policy.

	Name	Roles and Responsibilities
1.	**SGJ Leadership Team (Senior Management)**	• Function as Data Owners for the personal and sensitive data processed within respective LoB. • Function as Information Owner for information within units/department/LoB/Division. • Create the environment to facilitate adherence with this policy. • Review and approve this policy ensuring balance with achieving business objectives.
2.	**Data Governance Committee (DGC)**	• Identify classification policy requirements based on business needs. • Identify and communicate data governance and classification policy gaps for amendment or development of new policies. • Review and approve data classification policy. • Communicate this policy to team members and ensure that employees receive appropriate training regarding this policy.
3.	**Team Members**	• Handle all data in accordance with this policy and classification guidelines. • Immediately report any accidental or malicious breach of this policy to the appropriate department. • Report any identifiable gaps for policy update.
4.	**Data Custodian**	• Manage access rights to data according to the Data Classification Policy. • Implement controls to ensure the integrity, security, and privacy of data in accordance with classification levels.

	Name	Roles and Responsibilities
5.	**Data Steward**	• Consult with and support the Data Custodians with implementing data classification for systems and applications within their Line of Businesses (LoBs). • Provide input for the development and update of the Data Classification Policy. • Ensure that the policy aligns with business requirements and regulations. • Fostering awareness of the proper utilization of the Data Classification Policy within the business.
6.	**Legal Counsel**	• Manage the submission, review and approval process with the Ethics Review & Corporate Governance Committee and the SGJ Board. • Review third-party nondisclosure agreements and provide guidance on how such third-party data should be classified and handled internally. • Provide input on the classification of data from a legal perspective.
7.	**Data & Analytics Department**	• Develop Data Classification policies based on regulatory requirements and business needs presented by the DGC. • Present the Data Classification policy to the DGC for periodic reviews and updates. • Enforce Data Classification policies within the Group's enterprise data warehouses. • Apply classification levels on Group's metadata manager as required.
8.	**IT Department**	• Support data classification technologies that make possible the implementation of this policy. • Support the infrastructure and security technologies that make possible the implementation of classification guidelines. • Enforce the Classification Policy across relevant systems.

	Name	Roles and Responsibilities
9.	**Information Security**	• Manage and implement security technologies which are used to support data classification and other control tools associated with it. • Provide oversight for the management of Sagicor Jamaica Group's information resources. • Consult with the DGC to mediate high level data conflicts and discrepancies among the interest of the Data Trustees, Sagicor's Executive team and the needs and interest of other stakeholders. • Ensure data and information assets are handled according to classification guidelines, including with regards to the timely retention and disposal of data.
10.	**Internal Auditing**	• Conduct periodic reviews and audits to assess alignment of business operations with the policy. • Conduct periodic reviews and audits to assess gaps in the policy and make recommendations for improvement.
11.	**Data Protection Officer (DPO)**	• Periodically validating that the classification schemes serve its purpose. • Provide input for review and approval of the Data Classification Policy in alignment with privacy regulations.
12.	**Privacy Risk Officer**	• Provide input for the development of the policy and ensure risk levels translates into accurate classification schemes in alignment with regulations. • Align with the Information security and IT department to determine classification requirements.
13.	**Records Management**	• Ensure that data classification, standards or guidelines are enforced in accordance with this policy.
14.	**Enterprise Risk Management & Group Compliance Department**	• Monitor compliance with this policy. • Conduct risk management in alignment with the policy

Table1- Classification Policy Roles and Responsibilities

3 TERMS AND DEFINITIONS

3.1 The following definitions shall apply to this policy:

Key Definitions	
Data	A collection of facts generated in conducting business with our clients and stakeholders.
Data Classification	The process of organizing information assets using an agreed-upon categorization and risk level assessment.
Information	Data that has been processed, organized, interpreted and used for decision-making.
Third parties	A person/entity that is not a principal party of nor an affiliate of SGJ.
Jamaica Data Protection Act (JDPA)	The Jamaican Data Protection Act aims to safeguard the privacy and personal information for Jamaicans. It gives rights to residents of Jamaica and outlines obligations of all entities who manage, control, disseminate, or process data.
Data Governance Committee (DGC)	The Data Governance Committee consists of an executive representation from each LOB with an elected DGC Chair from among the LOB representatives. The DGC is responsible for policy setting, providing strategic direction for Data Governance programs and initiatives to meet the Group's business objectives.
Data Subject	A data subject is a named or otherwise identifiable individual who is the subject of personal data.
Information Owner	A Senior Manager with responsibility for the information (example, manuals, policies, reports etc.) within the care of their department, division or Line of Business.
Data Owner	A Data Owner is Senior Manager or Executive within a department, division or Line of Business entrusted with authoritative rights over the personal data being processed within said department, division or Line of Business. Note that DGC members function as Data Owners for the personal and sensitive personal data processed within their respective LoB. Ownership comes with responsibilities, as owners determine the purpose for data collection, define access rights, and establish retention periods.

Table 2-Terms and Definitions

4 DATA CLASSIFICATION PRINCIPLES

4.1 This policy is based on the following set of core principles that must be considered when classifying data:

4.1.1 Open and Transparent

Classification should be applied only if the nature or sensitivity of the data requires it. Access restrictions should only be chosen in cases where the information may be detrimental to a valid interest of the business, our clients and team members or third parties. This is to prevent over-classifying information which can lead to transparency and trust issues and deprive stakeholders' access to information required for decision making.

4.1.2 Risk Assessment

A risk assessment must be considered when classifying data. This will protect Sagicor Group Jamaica against potential risks. The risk assessment also sets out the appropriate measures to determine the severity and likelihood in case data is compromised.

4.1.3 The Lifecycle Approach

Data goes through different stages such as: creation, storage, use, share, archive and destroy. Consideration should be given throughout its lifecycle as classification may change according to the stage in which it is located. Data must be reviewed, evaluated and if required re-classified at each stage of the lifecycle.

4.1.4 Proportionality

The data classification process should ensure that information is classified to an appropriate level, which is as low as possible, but as high as necessary.

4.1.5 Data Governance

Data Governance plays a pivotal role in the classification process. This will ensure the success of data classification within SGJ and provides the framework for implementation and adoption across the Group. This further ensures the process is implemented in accordance with established principles and best practices.

5 RISK LEVELS

5.1 Data classification categories are assigned the risk levels Critical, High, Medium, and Low. These risk levels indicate the severity of the adverse impact to the operation of the business that may arise due to unauthorized access, disclosure or compromise of the data.

Critical This governed data is deemed to be crucial to the successful execution of business processes and adherence to the company's goals around financial, regulatory, and legal compliance. Unauthorized access or compromise of this data can lead to significant financial, reputational and competitive advantage losses. As such, data classified as **Critical** will receive the highest level of oversight and monitoring, including metadata management, high-frequency data quality testing, access screening, and usage auditing.

High This governed data is deemed to be significant to the operations of key business functions of Sagicor. As such, data classified as **High** will receive an elevated level of oversight and monitoring, including capture of an appropriate level of metadata, frequent data quality testing, and an appropriate level of access screening and usage auditing.

Medium This subset of data is deemed to be of importance, but not key to business functions within Sagicor. As such, data classified as **Medium** will be subject to periodic oversight and monitoring, including capture of a minimal set of metadata, infrequent data quality testing, and lowered levels of access screening and usage auditing.

Low This category of data is deemed to not be important to business functions, but nonetheless should be defined and governed within the company. As such, data classified as **Low** may not be subject to oversight and monitoring. Additionally, low risk data will have a reduced level of metadata collected when compared to other categories. It is important to

note that low risk data may not ever be the subject of data quality testing and may have no access screening and usage auditing.

5.2 Data that includes more than one category of data (example confidential and restricted) must be assigned the highest categorization and associated risk level. For example, a document that includes both confidential and restricted data, must be assigned a categorization of restricted and a risk level of critical.

6 DATA CLASSIFICATIONS

6.1 DATA CLASSIFICATIONS

6.1.1 The Data classification categories outlined in this policy identify how data should be classified regardless of format (for example digital files or hardcopy) or how it is stored (for example databases, filing cabinets etc.). It is important that employees and stakeholders recognize and understand the risk levels how each data category must be treated.

6.1.2 The classification categories are: public, Sagicor internal, confidential, sensitive, and restricted for the purpose of this policy.

6.1.3 The default classification shall be “Sagicor Internal.” All data should be considered to be at the “internal” classification, unless otherwise labeled or explicitly stated.

Data Category	Definition	Example (s)	Risk Level
Public	This information has been specifically approved for public release by Sagicor, unless already in the public domain. Unauthorized disclosure of this information will not cause any adverse impact. Disclosure of Sagicor's information to the public requires the existence of this label, the specific permission of the information owner, or the long-standing practice of publicly distributing this information.	(a) Marketing/advertising brochures and material posted to the Sagicor's website and social media platforms (b) Press releases (c) Job postings (d) Published annual reports	Low
Sagicor Internal	This information is intended for use within Sagicor only. Unauthorized disclosure of this information to outsiders may be against laws, regulations or company policies. Releasing Internal information may cause problems for Sagicor clients, its business partners or stakeholders. This type of information is already widely distributed within Sagicor, or it could be so distributed within the organization without advance permission from the information Owner.	(a) Sagicor's internal directory (b) Internal emails (c) Policies (d) Employee guides/training materials	Medium
Confidential	**Confidential Corporate Data** - This information is private in nature and should only be accessed by those with a legitimate business need. Unauthorized disclosure of this information to people without a business need for access may be against laws, regulations or business policies. Releasing confidential information may cause significant problems for clients, and business stakeholders. Decisions about the provision of access to this	(a) Business plans (b) *** Contracts and legal documents (c) Personnel files (d) Marketing strategies (e) Product plans (f) Project plans (g) Feasibility studies (j) Internal audit reports (k) Client financial details (example account balance) ***Note:*** *** *Contracts and legal documents can be confidential or*	High

Data Category	Definition	Example (s)	Risk Level
	information must be cleared through the information Owner.	*sensitive depending on the verbiage used in such documents.*	
	Confidential Personal Data— (a) means information (however stored) relating to— (i) A living individual; or (ii) An individual who has been deceased for less than thirty (30) years, who can be identified from that information alone or from that information and other information in the possession of, or likely to come into the possession of, Sagicor and (b) includes any expression of opinion about that individual and any indication of the intentions of Sagicor or any other person in respect of that individual. Authorization for the sharing of or access to personal data must be cleared by the Data Owner.	(a) Name (b) Date of Birth (DOB) (c) Residential Address (d) Tax Registration Number (TRN) (e) Mobile number (f) Mother's maiden name (g) Employee records (h) CCTV footage ***For the purpose of classifying data across the Group, Personal Data is considered a subset of Confidential data and should be so labelled.***	
Sensitive	**Sensitive Corporate Data** means data that is not defined as sensitive according to the Jamaica Data Protection Act but is considered and treated as sensitive based on the operations of the organization. This data, if exposed compromises the integrity and reputation of the organization and increases the liability of fraud to clients. Authorization for the sharing of or access to sensitive corporate data must be cleared by the	(a) Strategic Plans (b) Trade secrets (c) *** Contracts & legal documents (d) Financial records (e) Intellectual property (f) Employee information ***Note:*** *** *Contracts and legal documents can be confidential or*	Critical

Data Category	Definition	Example (s)	Risk Level
	Information Owner and the most Senior Executive for that division or Line of Business while others (Eg. Trade Secrets, Intellectual Property documents) may also require legal clearance.	*sensitive depending on the verbiage used in such documents.*	
	Sensitive Personal Data means personal data consisting of any of the following information listed 'a' through 'g' relating to a data subject as outlined by the Jamaica Data Protection Act. Sensitive Personal Data must only be shared with those authorized to access this data in the execution of their job function in service of the Data Subject. Authorization for the sharing of or access to sensitive personal data must be cleared by the Data Owner.	(a) genetic data or biometric data; (b) filiation, or racial or ethnic origin; (c) political opinions, philosophical beliefs, religious beliefs or other beliefs of a similar nature; (d) membership in any trade union; (e) physical or mental health or condition; (f) sex life; (g) the alleged commission of any offence by the data subject or any proceedings for any offence alleged to have been committed by the data subject. *Note that Personal Health Information (PHI) falls within this category.* .	Critical
Restricted	Data / Information that is very sensitive and is only available to a specific group, top management or limited number of team members. Typically, this would be information that if lost, damaged, or disclosed to unauthorized persons could lead to significant adverse impact, financial loss or penalties.	(a) Statutorily protected and sensitive information (b) Corporate information such as strategic corporate plans/ financial information (c) Merger and Acquisition information (d) Fraud and security investigation reports and findings. (e) Cryptographic keys information. (f) Banking details (debit card information, credit card) number and CVV2. (g) System vulnerability, audit, and compliance reports.	Critical

Table 3- Data Classification

7 POLICY DETAILS

7.1 Changing Data Classifications

7.1.1 Changes to the data classification must not violate regulations and governing business processes and policies.

7.1.2 The Data Owner must authorize changes to classification categories.

7.1.3 Updated classification categories should be reflected across systems where applicable.

7.2 System Implementation of Data Classification

7.2.1 Necessary technical measures must be taken to protect data and information classified as Confidential, Sensitive and Restricted to prevent unauthorized access throughout its lifecycle.

7.2.2 Necessary technical measures must be taken to limit or prevent data and information classified as Internal from being shared externally.

7.3 Data Access

7.3.1 Written authorization must be sought from Information/Data Owner for access to data or information for which they are responsible (unless such data is classified as public).

7.3.2 Appropriate contracts and non-disclosure agreements must be in place for third party access to confidential and sensitive data.

7.3.3 Third party vendors processing Sagicor's data must undergo a vendor assessment in accordance with Sagicor's Information Security Policy.

8 REVIEW OF POLICIES

8.1 The Data Classification Policy shall be reviewed annually or whenever there is a significant change in Sagicor's operations or external regulatory requirements to ensure continued suitability, adequacy and effectiveness.

9 EXCEPTIONS

9.1 Exceptions to this policy are approved by the Data Governance Committee (DGC) only under special circumstances and are granted for a specific period of time.

9.2 A formal request must be made in writing to the Data Governance Committee (DGC). This should outline the reason for the request supported by any additional relevant documentation. As per Section 1.4 of this Policy, Senior Management must also respond in writing before any exception is valid.

10 EFFECTIVENESS CRITERIA

10.1 Sagicor's Data Classification Policy will be effective in protecting the Group's data and information if the following criteria are met:

10.1.1 Classification categories and risk levels should be written in plain language that is easily understood.

10.1.2 Stakeholders should only have access to data or information based on the data categories outlined in this policy that applies to their job function.

10.1.3 Sagicor must ensure that new and existing data is categorized according to appropriate data categories and risk levels. This is important for compliance and legal obligations.

10.1.4 The policy should be communicated to all team members and should outline the Data Classifications and associated risk levels.

10.1.5 Appropriate technical measures should be taken to ensure compliance with this policy.

10.1.6 All team members are required to comply with the Data Classification Policy. Any team member found to be in breach of this policy will be sanctioned according to Sagicor Group Jamaica's disciplinary code.

11 POLICY COMPLIANCE

11.1 Failure to comply with this policy may result in disciplinary action in accordance with the Human Resource Management Policies and Procedures Manual.

12 APPENDIX

12.1 Related Policies/Forms

This section indicates all forms, policies and documents related to this policy.

12.1.1 Risk Category Abbreviations

The abbreviations outlined can be used for labelling purposes in systems, applications or databases:

Data Category	Risk Level	Abbreviation (For labelling purposes)
Public	Low	P
Internal	Medium	I
Confidential Corporate Data	High	C
Confidential Personal Data	High	Cpd
Sensitive Corporate Data	Critical	S
Sensitive Personal Data	Critical	Spd
Restricted	Critical	R

Table 4- Data Classification Abbreviations

12.1.2 Other Relevant Policies

Item/ Policy	Relevance
Data Privacy Policy	The purpose of this policy is to set out the means by which we comply with our obligations under the Data Protection Act (DPA) and the means by which we protect personal information relating to data subjects. This includes our obligations as to the collection, processing, transfer, storage, and disposal of that personal data.
Individual Critical Data Elements (CDEs) Policy	To guide SGJ's handling of clients' data to ensure compliance with regulations while simultaneously improving the data quality within SGJ's core and sub systems. This will facilitate innovation and the creation of value-added products and services to our clients. It will also create opportunities to exceed expectation in delivering exceptional client experience. It is an enabler in increasing the competitiveness of SGJ. The policy is a unified approach to ensure that the efforts by the Group to clean and manage data are transparent.

SGJ Information Security Compendium 2023	The Information Security Policies provides a security framework that will ensure the protection of Sagicor Group Jamaica information from unauthorized access, loss or damage while supporting the information-sharing needs of its dynamic culture. This policy can be accessed (https://sgjintranet/Viewer/viewer.html?file=/Content/documents/manuals/Information_Security_Compendium_2023.pdf#page=1&zoom=auto,-82,792).

Table 5- SGJ Relevant Policies

Note: This policy must be read in-line with all relevant policies including SGJ's Enterprise Risk Management [ERM] Policy.