Public broadcasting

PORTAGE GROUP CODE OF ETHICS & CONDUCT

Version: 2.3

Date of Approval by the CEO: 2026-11-02

Notes to readers

- This code applies to our employees, suppliers, consultants, directors and others.

Version tracking

Version	Date	Description	Editors	Approver
1.0	2022-08-23	Integration of our former Board of Directors' Code of Conduct with current best practices.	Maud Soulard, Compliance and Risk Management Director	Notarius Executive Committee
2.0	2023-09-14	Withdrawal from section 7.1 of Fatima Ba, Accounting Manager and HR Advisor	Maud Soulard, Compliance and Risk Management Director	Notarius Executive Committee
2.1	2026-06-12	Uniformity and consolidation of the Company's group codes of ethics, in line with our SOC2 certification.	Maud Soulard, Compliance and Risk Management Director	Portage Group CEO
2.2	2026-11-25	Inclusion of the concept of environmental responsibility	Maud Soulard, Compliance and Risk Management Director	Portage Group CEO
2.3	2026-11-02	Annual Review – Addition of Responsible Use of Artificial Intelligence (AI)	Maud Soulard, VP, Compliance and Risk Management	Portage Group CEO

Intellectual property

This Code of Ethics & Conduct is the exclusive property of the Portage Group.

No part of this document may be reproduced in any form or by any means without the prior written permission of the author.

For any reproduction, follow the CC BY-ND 4.0 standard of Creative Commons, i.e.: without modification and in its entirety with attribution of our copyright and mention of our company name.



© 2026 Portage Group

Table of contents

1 General Provisions 4
2 Scope and Duration of the Code 4
3 Our commitment 5
4 Definition 5
5 Our core values: 6
5.1 Trust 6
5.2 Respect 6
5.3 Ambition 6
5.4 Collaboration 6
5.5 Engagement 6
5.6 Empathy 6
6 Rules of Conduct and Obligations 7
6.1 Confidentiality and information security 7
6.2 Integrity and Business Ethics 8
6.2.1 Respect in the Workplace 8
6.2.2 Professional Competence and Quality of Work 9
6.3 Use of Electronic Communications and IT Tools 9
6.3.1 Social Media 10
6.3.2 Responsible Use of Artificial Intelligence 10
6.4 Drugs and Alcohol 10
6.5 Conflicts of Interest, Benefits and Gifts 11
6.6 Respect Others and Prevent All Forms of Harassment 12
6.7 Environmental Responsibility and Climate-Related Actions 13
7 Code Enforcement and Disciplinary Process 13
7.1 Interpretation of the Code 13
7.2 Right of Verification 14
7.3 Breach of the Code and duty to report 14
7.3.1 Who to Report a Breach to 14
7.3.2 Procedure 15
7.4 Responsibilities 16
7.4.1 Directors/Shareholders 16
7.4.2 Managers 17
7.4.3 Employees 17
7.4.4 Consultants & Suppliers 17
7.4.5 Chief Executive Officer 18
7.5 Measures in the Event of Breaches of the Code 18
7.6 Code Review and Approval 18

1 General Provisions

A word from our CEO

Ethics are at the heart of our values and guide our every action. As a Group, we support government institutions and regulated industries in securing their digital ecosystems by placing users at the heart of our approach. This commitment is based on integrity, responsibility and excellence, principles that guide our day-to-day decisions.

This Code of Ethics and Good Conduct defines the fundamental principles that must guide our behaviour and our choices. It is an essential reference for ensuring responsible governance and maintaining high standards of professional ethics. We are counting on every one of you - colleagues, employees, consultants and suppliers - to embody these values and contribute to the Group's reputation through exemplary conduct.

Don Cuthbertson
Signed with ConsignO Cloud (2026/11/02)
Verify with verifio.com or Adobe Reader.

_____

Don Cuthbertson

2 Scope and Duration of the Code

The purpose of this Code of Ethics (the "Code") is to establish a standard of conduct for all our directors, officers and employees in order to continue to uphold the Group's reputation for integrity, quality and ethical behavior. This Code also applies to our suppliers, subcontractors and business partners. Certain provisions or special measures may continue to apply after the end of employment. These provisions concern, among other things, the confidentiality of information. It defines the guiding principles that frame our behavior and decisions to ensure professional conduct, integrity and compliance with applicable laws and regulations, including ISO 9001, ISO 27001, SOC2 and Canadian legislation

Any entity wishing to collaborate with us must adhere to the same standards of integrity, regulatory compliance and respect for ethical principles that guide our activities. We expect our partners to comply with current standards of security, confidentiality and data protection, particularly those relating to the products we sell. Failure to do so may result in a review or termination of the business relationship.

This Code supplements the Group's Privacy Policy, the Terms of Use for our products and our contractual commitments. This Code also supplements the Group's internal Policies and Directives for the use of its employees or consultants where applicable.

We expect everyone with whom we do business to respect our values and ethical standards. This Code therefore also applies to visitors, consultants working both in our offices and remotely, and persons bound by a Professional Services Agreement or seconded to us by suppliers, with any necessary adaptations. Each person must take cognizance of these terms and conditions and comply with them at all times.

3 Our commitment

The Group is committed to:

- Respect the highest ethical standards.
- Ensure confidentiality and security of information.
- Prevent and deal with conflicts of interest.
- Promote a respectful, inclusive and harassment-free work environment.
- Comply with all applicable laws and regulations, including Act 25 on the protection of personal information and anti-corruption laws.
- Act with honesty, integrity and professionalism in all business transactions.
- Ensure that our partners and suppliers also respect these commitments.

4 Definition

The terms used in this Code are defined as follows:

- Alcohol: refers to any consumable substance with an alcohol content of more than 0.5% by volume.
- Benefit: means any tangible or intangible property of value, offered or conveyed by one person to another person or to a member of his or her family, including all types of gifts and hospitality. Without limiting the generality of the foregoing, benefits may include goods and merchandise, meals (including beverages), travel, accommodation and entertainment (tickets to concerts and sporting events, access to dressing rooms, VIP lounges and the like).
- Code: the present Group Code of Ethics and Conduct as updated from time to time.
- Executive Committee: designates the Group's designated managers appointed to the Board.
- Conflict of interest: Refers to any situation where our personal interests or those of a related person have or could be perceived to have an influence on our professional judgment, objectivity, independence or loyalty concerning the Group's interests.
- Consultant: a person whose services have been retained by the Group, either directly or through a third party, for a specific project or mandate.
- Discrimination: refers to situations where one or more people are treated differently or negatively because of their personal characteristics, beliefs, national or ethnic origin, culture, religion, political convictions, age, mental or physical disabilities, sex, sexual orientation, gender identity or any other reason prohibited by law.

- Drug: any substance, chemical or agent the use or possession of which is illegal or requires a prescription or personal authorization from a licensed medical practitioner, or the use of which is regulated by law.
- Employee: refers to any member of the Group's staff, including managers, regardless of employment status (temporary, permanent, casual, trainee or student).
- Supplier: refers to any third party who supplies goods or services to Portage CyberTech Group in compliance with contractual agreements signed between the parties.
- Group: refers to the Quebec company Portage CyberTech Inc. and all its affiliated companies including 10084182 Canada Inc. O/A Becker-Carroll, Vivvo, Solutions Notarius Inc., 1CRM and OPIN Digital.
- Stakeholder: refers to a person or organization that may affect, be affected by or expect to be affected by a decision or activity (such as employees, customers, suppliers, communities, investors, shareholders, etc.).
- Person: means any natural person or legal entity, as referred to in this Code.
- Personal information: means any information concerning a natural person.

5 Our core values:

Our values characterize our actions and conduct. They guide us in our dealings with employees, customers and stakeholders.

5.1 Trust

We uphold security & reliability in every solution.

5.2 Respect

We build trust through respectful interactions, valuing each relationship and perspective within and outside our organization.

5.3 Ambition

We are driven by a strong desire and determination to achieve great things, pushing the boundaries of what is possible in technology and service.

5.4 Collaboration

We believe that working together enhances productivity and creativity, driving the success of our clients and our company.

5.5 Engagement

Our team is passionately engaged, bringing enthusiasm and dedication to every project and client interaction.

5.6 Empathy

We prioritize understanding and addressing the needs of our clients and team, fostering a supportive and cooperative work environment.

These core principles guide the Portage Group as we navigate the complexities of the modern digital

landscape, ensuring we deliver exceptional value and support to our clients while advancing our industry.

6 Rules of Conduct and Obligations

6.1 Confidentiality and information security

Treating information as confidential means not revealing its content without the owner's authorization. The nature of our work gives us access to information that may not be available to others. You are responsible for the security of documents and confidential information entrusted to us.

- Respect the Group's Confidentiality Policy and signed contractual agreements (e.g. suppliers undertake to ensure the confidentiality of information to which they have access as part of their business relationship with the Group).
- All confidential or privileged information must be protected and must not be shared without authorization.
- Compliance with cybersecurity protocols and data protection policies is mandatory.
- Any violation must be reported immediately to the compliance team.
- Employees must refrain from using information obtained in the course of their employment for personal purposes or to benefit a third party
- Balance "open communication" with the "need to know and share".
- Exercise caution and reserve in disclosing anything that comes to your knowledge in the course of or in connection with the performance of your duties.
- Protect proprietary and confidential information when you are in a public place (e.g., on an airplane, in a restaurant or in an elevator) by avoiding open discussion and limiting the use of electronic communication devices.
- Meet your confidentiality commitments to customers.
- Respect the confidentiality of Group information
- Keep securely all documents obtained or received in the course of your duties and, where applicable, dispose of them in a similarly secure manner.
- Do not disclose confidential information unless necessary, with official permission, or where a legal right or obligation to disclose exists.
- Think about data confidentiality at the start of any new project or initiative (internal or with customers) that will require the use of personal data, by carrying out a confidentiality impact assessment.
- Honour the property rights of others as expressed in patents, trademarks and copyrights.
- Respect and comply with policies and legislation on the protection of personal information and privacy.
- As a director, you may not, during your term of office or after its expiry, use for your benefit, or for the benefit of anyone else, any information or intelligence obtained because of your duties when it is or becomes confidential; you are required at all times to respect the confidential nature of any information or intelligence so obtained, except with the Group's prior written permission.

6.2 Integrity and Business Ethics

The Group's relationships with its customers are founded on honesty and credibility. You are therefore expected to act with integrity and diligence to uphold these principles. You must treat all customers equally, without. Integrity means applying the highest standards of professional conduct in all activities that affect our customers, colleagues and communities. It means behaving in a way that justifies public trust and strengthens the Group's reputation. It also means that we must be independent-minded, act objectively and exercise good judgment. Integrity refers to the independence and probity of the Group's employees, shareholders and consultants/suppliers in their decision-making based on our mission or the Agreements signed with us, the subordination of their personal interests to the value and importance of the position or role they occupy, and accountability and transparency in the performance of their duties. Suppliers must be honest, professional and fair in their business dealings with the Group, particularly regarding meeting their contractual obligations.

As such:

- The Group strictly prohibits any form of corruption, fraud or embezzlement.
- No gift or benefit may be offered or accepted if it influences a business decision.
- Any actual or potential conflict of interest must be declared to management.
- Decisions must respect the principles of fairness and transparency.
- Employees must refuse any request for inappropriate or illegal conduct, especially when interacting with government entities.
- Any involvement in anti-competitive practices is prohibited, including the unauthorized disclosure of sensitive market information.

6.2.1 Respect in the Workplace

By demonstrating integrity and professionalism in everything we do and say, we set ourselves apart from the rest. It is your responsibility to ensure that your decisions and actions respect our ethics and values above all else.

- The Group will not tolerate any form of harassment, discrimination or intimidation, whether towards a colleague, a supplier or any other business partner.
- We foster an inclusive and respectful work environment.
- Employees must report any inappropriate behaviour.
- Relationships between colleagues must be based on mutual respect and collaboration.
- Carry out your duties and obligations with honesty, integrity and professionalism.
- Be transparent in your actions and communications to build trust and minimize ambiguity.
- Place integrity above the desire for personal reward
- Be courteous in all your contacts; approach conflict and confrontation constructively.
- Acknowledge your mistakes and work quickly to rectify any negative consequences.
- Respect internal policies and procedures as well as the specific requirements of our customers.

6.2.2 Professional Competence and Quality of Work

Delivering quality professional services to customers requires that all our activities are conducted in compliance with all relevant standards, whether technical, professional or related to our external certifications. You are responsible not only for maintaining the highest standards in your own work, but also for drawing on our vast reservoir of knowledge and experience to provide excellent service to our customers.

- Provide customers with services that comply with Group policies and procedures.
- Comply with the directives, policies, procedures and contractual clauses that apply to you.
- Exercise an appropriate degree of due diligence in your work.
- If necessary, consult peers, specialists and other Group resources.
- Issue communications that meet the highest quality standards.
- Meet your commitments to customers without sacrificing quality and compliance.
- Foster an environment that encourages the sharing of ideas and knowledge.
- Exercise good professional judgment.
- Never stop expanding your knowledge and maintain an appropriate level of ongoing training.

Our managers have a duty to lead by example, to promote and encourage the principles of this Code. They must also help their teams understand the Code and answer any questions they may have about it. Our managers must accompany and support all those who may denounce behaviour contrary to the spirit of this Code.

6.3 Use of Electronic Communications and IT Tools

The use of IT resources must never be detrimental to work, information security, the operation of the IT and telecommunications network or the Group's image, nor must it be used for immoral or illegal purposes. Group employees must adhere to, undertake to respect and apply the *Group Security Policy* & *Employee Directive*, under penalty of sanctions.

Other persons to whom this Code applies undertake, in the performance of an Agreement or mandate or when present at our offices, to:

- The use of the Group's IT tools must comply with security policies.
- Personal use of IT resources must be limited and must not compromise data security
- It is forbidden to use company equipment for purposes that are illegal or contrary to Group values.
- All use of electronic communications and social networks in connection with the Group must comply with the principles of responsibility and professional ethics.
- Do not use personal e-mail accounts for business communications.
- Not to pass on or share login details for Group IT tools, including access card codes, if applicable.
- Do not modify or deactivate security or other settings.
- Not to access, send, post or store pornographic or other indecent or offensive material when using or accessing the Group's IT or communication tools. Not to connect to online gambling sites or

engage in illicit activities while performing your duties for the Group.

- Do not store or transmit images or multimedia files, generate high-speed network traffic or incur data storage costs for personal use.

6.3.1 Social Media

When using the Internet and social media, whether in a personal capacity or when doing so on behalf of the Group, a supplier or otherwise, you must not contravene any law and must not make any abusive, defamatory, racist or sexist comments or transmit any hateful, pornographic or harassing material or material in respect of which the Group does not hold the copyright. As such, the Group reserves the right to remove such content at its sole discretion and without prior notice. Any opinions you wish to share on our website, or our social media must be shared respectfully without personal attack. In the language of the Internet, capitalization is equivalent to shouting and can be interpreted as aggressiveness, which is unpleasant for other readers. Any message containing a capitalized word (apart from acronyms) may be rejected. Suppliers must obtain the Group's prior written approval before commenting on or promoting the Group's business. This requirement applies to all advertising media, as well as to print, electronic and other media.

6.3.2 Responsible Use of Artificial Intelligence

Portage Group recognizes the opportunities offered by artificial intelligence (AI) to support innovation, efficiency, and the quality of its operations. However, its use must comply with the principles of ethics, transparency, accountability, and information security that guide the Group.

Any person using artificial intelligence tools or systems in the course of their duties must:

- Use only tools and services authorized by the Group, in accordance with applicable internal policies and guidelines.
- Protect the confidentiality of information, personal information, and intellectual property rights. No confidential or sensitive information, or information belonging to a client or third party, may be disclosed to an AI tool without appropriate authorization.
- Exercise sound judgment and perform appropriate human review of AI-generated outputs, particularly when such outputs may influence a decision, a contractual commitment, or an individual's rights.
- Refrain from using AI for deceptive, discriminatory, fraudulent, or other purposes contrary to the Group's values and obligations.
- Remain accountable for work, decisions, and communications carried out with the assistance of AI.

The use of artificial intelligence does not relieve any person of their professional, legal, contractual, or ethical obligations.

6.4 Drugs and Alcohol

The Group is committed to providing a healthy, safe and supportive work environment for its employees. Whether in an administrative setting or in technological development, we implement measures to reduce

risks to physical and mental health, notably by promoting ergonomic working conditions, work-life balance and the prevention of psychosocial risks.

Security in the workplace also includes the protection of data and information systems. Every employee must apply good cyber-security practices and respect the protocols put in place to prevent any incident that could compromise the integrity of information.

At the same time, it is essential that everyone is fit to perform their duties safely and professionally. The use of alcohol, drugs or any substance that could impair concentration or judgment is strictly forbidden during the performance of

All persons to whom this Code applies therefore undertake not to consume drugs or alcohol that could lead to them being impaired on the Group's premises, either in person or by videoconference.

The purchase or sale of drugs or alcohol is strictly forbidden.

Anyone behaving in a way that suggests the influence of alcohol or drugs is liable to be immediately removed from his or her position or mandate, and to be tested and investigated as appropriate.

The consumption of alcoholic beverages on Group premises may only be permitted, under certain conditions, by a member of senior management.

Finally, any direct or indirect association with or participation in the activities of a criminal organization, including but not limited to trafficking in drugs and other illegal substances and laundering the proceeds of crime, is strictly forbidden.

6.5 Conflicts of Interest, Benefits and Gifts

Conflicts of interest - whether real or perceived - arise when professional judgment is affected by outside influences. They can prevent us from doing the right thing, or lead people outside the Group to doubt our intentions. You have a responsibility to avoid conflicts of interest by ensuring that your business decisions, transactions and/or relationships do not place your personal interests ahead of those of the Group, its customers, your colleagues or the public.

Suppliers/consultants must exercise due care and diligence to prevent and promptly declare any conflict of interest or appearance of conflict of interest. All forms or attempts of bribery, extortion, bid-rigging, influence peddling, malicious or unauthorized obtaining or sharing of privileged information, embezzlement, falsification and other fraudulent practices are strictly prohibited. They must not place a Group employee a situation that could compromise his or her integrity or ethical behaviour, or that could be perceived as doing so, by offering any goods, meals, favours, services, advantages, cash payments, invitations or gifts.

- Do not confuse Group assets with your own, and do not use them for your own benefit or for the benefit of third parties. Similarly, outside the scope of your duties or mandate, the use of Group resources for personal purposes or for the benefit of third parties is prohibited.
- Adopt an impartial stance in the face of any influence or appearance of influence exerted by conflicting interests.
- Avoid any external activity, situation or relationship that could affect, in fact or in appearance, your professional judgment.
- Use your discretion before taking part in personal social activities involving customers.
- Immediately inform the COO in writing of any personal or professional relationship that may give rise to a real or perceived conflict of interest.
- Avoid any outside employment that might conflict with your responsibilities to the Group or harm its interests.
- As a director, you must not, during your term of office or after its expiry, intervene in the name or on behalf of a third party in any procedure, negotiation or transaction involving the Group and in which you hold information that is not accessible to the public.
- As a director, you are prohibited advising to customers based on non-public information about the Group.
- Do not accept gifts, hospitality, gratuities or other benefits of any kind, unless they are customary and of little value.
- Suppliers are prohibited from offering gratuities to a third party or to a Group employee to influence a decision in favour of themselves or a third party.

6.6 Respect Others and Prevent All Forms of Harassment

The Group will never tolerate harassment by its shareholders, employees, suppliers, consultants, partners, customers or visitors. For its employees, the Group has adopted a *Policy for the Prevention of Psychological or Sexual Harassment in the Workplace* that meets the requirements of the CNESST and applicable Quebec and Canadian legislation. Suppliers undertake to treat Group customers, employees and partners with courtesy and professionalism. We will not tolerate any action, conduct or behaviour of a humiliating, intimidating or hostile nature.

Treat others with respect and avoid situations that could be perceived as inappropriate. The Group promotes diversity and inclusion in the workplace. Reactions, criticisms and challenges should always be expressed appropriately and respectfully. Always be aware of cultural sensitivities; what is acceptable in one culture may not be in another. It's important to be aware of these differences and to understand them.

Your responsibilities:

- Always treat others with respect.
- Respect applicable human rights legislation.
- Never intimidate or humiliate others, either physically or verbally.

- Refrain from making inappropriate jokes or comments.
- Don't display offensive or disrespectful material.
- Express your disapproval (see 7.2) if you observe hostile, intimidating, humiliating or disrespectful behaviour.
- Adopt responsible business practices that do not violate human rights.

6.7 Environmental Responsibility and Climate-Related Actions

The Group recognizes that environmental and climate-related issues may influence its organizational context, its interested parties, and its risk management activities, in accordance with the principles of ISO 9001 and ISO 27001. Accordingly:

- The Group is committed to complying with all applicable environmental laws and regulations in the jurisdictions where it operates.
- Operational and strategic decisions take into account, where relevant, reasonably foreseeable environmental impacts related to our activities, products, and services.
- The Group promotes responsible practices aimed at reducing significant environmental impacts, including the efficient use of resources, waste reduction, and the limitation of non-essential travel when compatible with our operational needs.
- Employees, suppliers, and consultants must avoid any action that could result in an unreasonable negative environmental impact or regulatory non-compliance.
- Any situation or activity presenting a potential environmental risk must be reported to the Chief Operating Officer or the designated responsible person.
- Any situation or activity presenting a risk related to climate change must be reported to the Chief Operating Officer or the designated responsible person.
- The Group encourages its partners to adopt professional practices that align with the principles of environmental protection and reasonable climate responsibility.

This provision aims to ensure responsible governance consistent with contemporary expectations in ethics, compliance, and sustainability.

7 Code Enforcement and Disciplinary Process

7.1 Interpretation of the Code

Any request for information or clarification concerning the application or interpretation of this Code should be addressed to legal@portagecybertech.com

When an interpretation of the Code is required, the Group COO is responsible for making a decision.

7.2 Right of Verification

The Group reserves the right to verify that all its employees, consultants, suppliers and others comply with the Code from time to time. The Group reserves the right to take appropriate action depending on the seriousness of the breach. Possible sanctions may range from a simple warning to the termination of current contractual agreements, or even dismissal in the case of employees. The Group reserves the right to notify the relevant authorities if required.

7.3 Breach of the Code and duty to report

Failure to comply with the letter and spirit of this Code and the Group's policies, procedures and guidelines will result in disciplinary action and possible dismissal. In addition, certain violations may result in legal action.
We must ensure that we respect and apply the requirements of the Code.

We must all report the following situations/behaviours in good faith:

- Any known or suspected violation of our Code or any other governance document.
- Any alleged breach of applicable laws or regulations.
- Any misconduct we witness or experience.
- Any pressure to compromise our ethical standards and good conduct.

The Group is committed to protecting whistleblowers against any form of reprisal. Indeed, no reprisals may be taken against a person for having, in good faith:

- Asked for advice on applying the Code;
- Asked for advice on making a disclosure;
- Make a disclosure;
- Collaborated on a disclosure audit;
- Refused to participate in a breach of the Code.

7.3.1 Who to Report a Breach to

All questions or requests for information concerning the application or interpretation of this Code should be referred to your immediate superior or the COO

If you have a complaint or concern about compliance with applicable law, this Code or any other Group policy, procedure or guideline, or if you are aware of any conduct, omission or practice that violates or may violate the letter or spirit of these provisions, you should communicate this information in good faith to the Ethics Contact (the COO) or your manager.

- If the report relates to a breach of privacy, please contact dpo@portagecybertech.com , or Don

Cuthbertson, Group President and CEO.

If the alleged breach concerns a member of the Board, you can write to the shareholder's director at the following e-mail address: ombudsman@portagecybertech.com

All complaints, concerns or statements will be handled promptly and confidentially.

Any information that could demonstrate that a breach has been committed, that a breach is about to be committed or that a member of staff has been asked to commit a breach may be disclosed.

Any person who discloses this Code that is deemed vexatious or made in bad faith is liable to sanctions.

The Group takes care to maintain adequate procedures for confidential reporting. Complaints, concerns or reports of actual or potential violations will be treated confidentially. No retaliation will be tolerated against any person who reports in good faith, or has reasonable grounds to report, a complaint, concern, violation or potential violation regarding this Code of Conduct or internal policies, procedures or guidelines, or in cooperation with an investigation of a violation or potential violation. Any person who retaliates against a complainant may be subject to disciplinary action.

7.3.2 Procedure

Employees considering making a disclosure may seek advice from the Ethics Officer or their manager. Employees who know of a breach of this Code, the manager of the employee concerned by a disclosure or members of the Group's senior management may also seek advice from the Ethics Officer. The Ethics Officer and managers ensure the confidentiality of their dealings with those who consult them.

- A breach of the Code must be the subject of a written complaint to the manager of the staff member making the complaint.
- A disclosure can also be made anonymously directly to ombudsman@portagecybertech.com
- To be admissible, a disclosure must specify:
    - The identity of the member(s) of staff, consultant(s) or supplier(s) who may have committed the breach, who may be about to commit the breach or who may have asked a member of staff to commit a breach;
    - Description of the alleged breach of this Code;
    - The date on which the breach was allegedly committed;
    - Whether the alleged breach has already been disclosed without effect, and to whom;
    - A copy of any document supporting the denunciation.
- If the application is deemed admissible, a written acceptance or refusal with reasons will be sent to the applicant within ten (10) working days of receipt of the application.
    - A breach disclosure audit may not be performed, or may be discontinued, if the COO or Manager believes that:
        - ✓ The disclosure is frivolous or vexatious, was not made in good faith or is not justified

by its purpose;

- ✓ The disclosure does not contain sufficient details regarding the alleged breach;
- ✓ The refusal or interruption of verification is appropriate for any other reason deemed valid, in particular in that the delay between the time of disclosure and the alleged breach is undue.

- If an audit is deemed necessary, a written notice specifying the purpose of the disclosure is given to the COO.
  - ✓ The person against whom an allegation of misconduct is made is informed that a disclosure audit is in progress and is met for this purpose by the COO accompanied by the notified manager.
  - ✓ Any staff member whose testimony is considered relevant to the disclosure audit may also be interviewed, if deemed useful.
  - ✓ The identity of the person making the disclosure, the witnesses interviewed and the person who is the subject of a disclosure are protected. The same guarantee of confidentiality applies to information and documents obtained or created in the course of a disclosure audit.

- At the end of a disclosure audit, the COO makes:
  - Report to the Board that a breach of the Code has occurred, or to the DPO if it involves personal information. This report may be accompanied by recommendations on appropriate measures to be taken, given the circumstances, after consultation with the Human Resources Department if necessary.
  - On the contrary, closes the file if the COO concludes that no breach of the Code has occurred. The COO notifies the whistleblower and the person against whom the disclosure was made in writing.
- The filing of a complaint under this Code in no way precludes the exercise of other legal recourses.

7.4 Responsibilities

Group employees and directors must demonstrate leadership and promote compliance with the Code.

7.4.1 Directors/Shareholders

At the start of each term of office, all directors must confirm in writing that they accept this Code and have read it. The application of this Code requires a personal commitment on the part of each director, at the start of each term of office, to adopt and respect the ethical values and rules set out in this Code, and to comply with each of its provisions. Directors must, at the start of each term of office and as required thereafter, disclose to the Group any interest they already have or subsequently acquire, either personally or through an associate, in a company, enterprise, association or network, where such interest is likely to place them in a conflict of interest situation; they must then abstain from taking part in and voting on any deliberations and decisions concerning the company, enterprise, association or network in which they have such interest.

He or she must also promptly notify the Group of any modifications or changes in this regard. At the start of each term of office, directors must confirm in writing that they will never disclose any confidential information or data concerning the Group, its customers, suppliers or employees, even after they have ceased to hold, unless such disclosure is authorized by the CEO of the Group, its customers, suppliers or employees.

7.4.2 Managers

Like employees, they adhere to the Code as soon as they start work. They ensure that all persons under their supervision are familiar with the Code and adhere to it. They also ensure that it is applied within their departments, and deal with any disclosure of misconduct or report of reprisals submitted to them in accordance with the provisions of this Code.

Managers ensure that their team members complete an annual declaration of integrity, impartiality and confidentiality.

7.4.3 Employees

- On hiring, employees sign the Consent document confirming that they have read and understood the Code, and that they agree to abide by its rules and fulfill the obligations it imposes.
- During employment, employees undertake to disclose to their manager any activity or event that may prevent them from complying with the Code.
- Every year, employees complete a form attesting to their integrity and impartiality in the performance of their duties, as well as to their respect for the confidentiality of the information they have acquired via a dedicated form.

7.4.4 Consultants & Suppliers

The Group's business partners and agents are expected to conduct themselves per the principles set out in this Code when interacting with us or acting on our behalf. They are required to respect our commitments to ethics and integrity, in particular by ensuring:

- Comply with applicable laws and regulations;
- Refrain from all forms of corruption, including the payment of bribes;
- Promote fair competition by complying with antitrust rules;
- Adhere to our commitment to human rights and worker protection;
- Contribute to a safe and healthy work environment.

All agreements with business partners and agents must comply with market standards and the principles set out in this Code, as well as with the Group's internal policies and procedures. In addition, our suppliers must comply with our Code of Conduct, which defines the minimum standards to be observed when supplying goods and services to the Group. It is the responsibility of each supplier to ensure that these principles are understood and applied by all those involved in their business with us.

- When Consultants are retained, they confirm in their Master Agreements or other Contracts with the Group that they have read and understood the Code and undertake to comply with it.
    - If the Consultant is a company, the latter undertakes to provide the Group with a copy of the Code to any person assigned to perform the services, and to ensure that such persons always comply with their obligations under the Code.
- In the event of major changes only, Consultants review the Code and renew their commitment to it, on a personal basis or on behalf of Employees assigned to perform services, as a condition for maintaining and continuing the Framework Agreement and contracts in force.

7.4.5 Chief Executive Officer

Receives reports following a disclosure audit and makes decisions, giving reasons for the application of the present Code.

7.5 Measures in the Event of Breaches of the Code

Those who contravene any of the provisions of this Code may be subject to the following sanctions, depending on the nature and seriousness of the offence:

- A reprimand;
- Delivery of the gift, donation or benefit received;
- The return of sums of money, benefits or goods received in contravention of the Code;
- A provisional statement with treatment;
- Suspension without pay;
- Termination of employment or dismissal.

7.6 Code Review and Approval

This Code will be reviewed and updated regularly to ensure its compliance with regulatory developments and best practices. A minimum annual review is in place.

The Code is approved by the Group's Chief Executive Officer (CEO), which also approves any amendments to be made.

The COO oversees the day-to-day application of this Code.