

CODE OF CONDUCT POLICY

The Policy is applicable to Fractal Analytics Limited and its subsidiaries in the jurisdictions in which the Company does business.

1. Purpose 4
2. Scope and application 5
3. Employee Responsibilities 4
4. Policy Section and Clauses 5
4.1. Compliance with Governmental Laws, Rules and Regulations 5
4.1.1. Competing Fairly 5
4.2. Acting with Integrity 5
4.2.1. Maintaining highest standards of Integrity 5
4.2.2. Conflict of Interest 5
4.2.3. Protection of Interest 7
4.2.4. Inducements 7
4.2.5. Bribery 7
4.2.6. Gifts and hospitality 7
4.2.7. Suspected Fraudulent behavior 8
4.2.8. Communication 8
4.2.8.1 Social Media 8
4.2.9. Maintaining Confidentiality of Information 8
4.2.9.1 Privacy and Data Protection 9
4.2.9.2 Information Security Guidelines for Data & Asset usage 9
4.3. Protection of Company Assets 12
4.3.1. Intellectual property 12
4.4. Maintaining an Equitable and Safe Workplace 12
4.4.1. Inclusion, mutual trust and respect 12
4.4.1.1 Non Retaliation Policy 15
4.4.1.2 Harassment 13
4.4.1.3 Prevention of Sexual Harassment 13
4.4.2. Equal Employment Opportunity 14
4.4.3. Health and Safety 14
4.4.4. Slavery and Human Trafficking 14
4.4.5. Under-age employment or Child Labor 14
4.4.6. Employee Grievance Redressal Mechanism 16
4.5. Code of Conduct Awareness, education, and training 14
4.6. Disciplinary Process 15

5. Responsibility to uphold the Code of Conduct 15
6. Special situations and exceptions 16
7. Enforcement 16
8. Review and Updates 18
9. Definition and Acronyms 17
Definitions 17
Acronyms 17

Document Control Section

Document Name	Fractal Analytics – Code of Conduct Policy
Abstract	Fractal Analytics policy to maintain a standard of conduct that is in accordance with the applicable laws, regulations, rules and with the highest standard of ethics and values.

Confidentiality Agreement

This document is copyrighted, and all rights are reserved. This document shall not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from an authorized representative of Organization. This document is for internal use only and shall not, in whole or in part, be provided to anyone outside of Organization, including customer, clients, or prospects.

1. Purpose

The purpose of this Code of Conduct is to establish a clear framework of ethical principles and behavioural expectations for all employees within our organization. At Fractal, we are committed to upholding the highest ethical standards while extending extreme trust. It is central to our culture and identity as an organization.

Our Code of Conduct has been designed to promote integrity, respect, trust and accountability, ensuring a positive and inclusive workplace culture. It encapsulates our values and people principles, which guide our actions and decisions everyday. By defining clear standards and guidelines, Fractal intends to create and foster an environment where diversity is valued, and every individual is encouraged to contribute to their fullest potential.

This document serves as a consistent framework for decision-making and interactions, enhancing trust and cooperation at all levels. It reflects Fractal's commitment to ethical behaviour and trust in its employees to maintain these standards. The purpose of this Code is to prevent misconduct and promote ethical business practices both within and outside Fractal.

2. Scope and Application

Code of Conduct applies to all full time employees, contractors, interns, vendors or any other individuals who are working at Fractal site, client site, working from home or anyone who has been given access to work within Fractal's network.

The document applies to Fractal Analytics and all its subsidiaries globally, to ensure consistency in expectations from all individuals associated with Fractal to uphold standard corporate values and people principles. It governs the appropriate usage of information that you have been given access to and any physical assets of Fractal which have been assigned to you.

3. Employee Responsibilities

Employees are expected to:

- Read and understand the code of conduct policy
- Adhere to the guidelines that have been outlined in the policy while carrying out their day-to-day activities.
- Comply with all applicable laws, regulations of the country/state where they are residing
- Comply with all company policies.
- Make all decisions in light of Fractal values, people principles and guiding principle which states that we will prioritise client before Fractal, Fractal before team, and team before self" in decision-making

We expect that by adhering to this Code of Conduct, all members of the Fractal community contribute to maintaining a secure, ethical, and high-trust environment that supports the company's mission and values. Fractal reserves the right to modify this policy from time to time as appropriate.

4. Section and Clauses

4.1. Compliance with Governmental Laws, Rules and Regulations

All employees, contractors, interns, vendors, and other individuals working at or with Fractal Analytics must comply with all applicable governmental laws, rules, and regulations. Employees are expected to acquire sufficient knowledge of legal requirements relevant to their roles to recognize potential dangers and violations. Non-compliance can lead to individual criminal or civil liability and may also lead to corporate civil or criminal liabilities, reputational damage, for the company. Any such violations that may expose the company to civil or criminal liability or loss of reputation and business may cause the company to take disciplinary action. It is encouraged that in case any individual associated with Fractal has a doubt regarding a action or decision, they should seek guidance from the Legal Department or their supervisors to ensure all actions comply with legal standards and Company policies. It is essential to maintain highest standards of legal compliance for protecting both individual and Company interests.

4.1.1. Competing Fairly

Fractal's success is built on the quality of services that we deliver. Avoid engaging in actions, behaviours, decisions that may create a perception of unfair competition. Fractal is committed to maintaining legal and ethical standards in competition. We encourage our employees to use all resources, knowledge, and expertise to their competitive advantage, but they must do so while respecting the integrity of free markets and the rights of others to conduct their business. No undue pressure should be exerted on clients, ensuring their freedom to choose between different service providers basis merit.

Collaboration with competitors on pricing, service decisions, or market strategies is strictly prohibited. Practices such as bid rigging, price fixing, and market allocation are prohibited and against our principles. Avoid collaborating or agreeing with competitors about pricing, market division, or timing of price changes.

We safeguard our confidential information and respect that of our competitors. Sharing Fractal's confidential information with competitors or accepting their confidential information is unacceptable. Furthermore, we must not misuse the confidential information of others, including previous employers.

If a competitor approaches you with prohibited propositions, clearly refuse to engage, reject any confidential information, and promptly report the incident the Legal team or whistleblower team.

Compliance with antitrust and competition laws is mandatory. Any individual found engaging in activities that violate any such laws shall face disciplinary actions as outlined in misconduct policy.

4.2. Acting with Integrity

4.2.1. Maintaining highest standards of Integrity

Employees must display the highest level of ethics and integrity in every sphere of activity and abide by the rules and regulations of the organization.

4.2.2. Conflict of Interest

Employees must avoid or declare conflicts of interest that may lead (or be seen to lead) to divided personal loyalties. All employees should nurture and protect Fractal's interests all the time. Any conflict of interest also includes conflicts between Fractal's interest and employee's interests outside Fractal. It could arise from employee having

a large shareholding in a competing company, participating in the business and management of another company in any manner, spending Fractal time on other things, or acting as a supplier or competitor to Fractal.

All employees should remain independent in any decision that they may be required to take and should disclose any interest – personal, professional, academic or business – which may arise directly or indirectly through their relatives that may conflict with their responsibilities.

NOTE: IN THE EVENT OF ANY DOUBT PERTAINING TO CONFLICT, EMPLOYEES SHOULD DISCUSS WITH THEIR MANAGER and HCBP for appropriate counsel.

An Employee involved in any of the types of relationships or situations described in this Code should immediately and fully disclose the relevant circumstances to his or her manager. Failure to disclose facts shall constitute grounds for potential disciplinary action.

(i) Outside Work / Outside employment

All employees of the company shall devote themselves exclusively to the business of the company. They are not to take up any other work/assignment for remuneration (part time or otherwise including weekends) or work on advisory capacity or be interested either directly or indirectly (except as shareholder or debenture holder) in any other trade or business during your employment with the company without prior approval in writing. It is important to check with the HCBP and get prior written approval from Business Leader or CPO to ensure there are no conflicts of interest.

(ii) Outside Directorships

It is a conflict of interest to serve as a director of any company that competes with the Company. Employees must obtain prior written approval from the CEO before accepting a directorship. Such approval is discretionary, may be conditioned upon the completion of specified actions.

(iii) Business Interests

If employees are considering investing in the Company clients, supplier, developer or competitor, they must first take great care to ensure that these investments do not compromise their responsibilities to the Company. Many factors should be considered in determining whether a conflict exists, including the size and nature of the investments; their ability to influence the Company's decisions; their access to confidential information of the Company or of the other company; and the nature of the relationship between the Company and the other company.

(iv) Personal Conflict of Interest/ Related Parties (Family and personal relationships)

As a general rule, employees should avoid conducting Company business with a relative, or with a business in which a relative is associated in any significant role because in such situations, our own personal interests may affect our ability to act in Fractal's best interests or may compromise our ability to remain objective. For the purpose of this policy, the definition of Relatives include spouse, siblings, children, parents, grandparents, grandchildren, aunts, uncles, nieces, nephews, cousins, step relationships, and in-laws. Employees must not engage in activities that compete with Fractal's interests, either directly or indirectly or use the company's resources for personal gain. This includes avoiding the use of Fractal's property or information for personal advantage or that of family and friends. Any opportunities discovered through Fractal's resources must not be pursued for personal benefit. Maintaining these standards ensures the integrity of our professional conduct and protects the value of Fractal's assets.

Such conflicts of interests may present itself in several different situations. Hence it is important to consult legal team in case of any situation that you think may result in actual, potential or perceived conflict of interest. Whenever, presented with such instances of personal conflict of interest, proactive disclosure of the same is the first step to ensure that required approvals are obtained, required restrictions can be enforced.

The Company discourages the employment of relatives in positions or assignments within the same account team and prohibits the employment of such individuals in positions that have a financial or other dependence or influence (e.g., an auditing or control relationship, or a supervisor, skip manager, Team Lead/subordinate relationship).

The purpose of this policy is to prevent the organizational impairment and conflicts that are a likely outcome of the employment of relatives or significant others, especially in a supervisor, skip manager, Team lead/subordinate relationship. If a question arises about whether a relationship is an instance of personal conflict of interest, please disclose the details of the same to your HCBP, the shared responsibility for determining whether an Employee's acknowledged relationship will result into violation of the conflict of interest clause is held by the Human Capital team and Legal team. the decision will be objectively made based on facts and communicated to the employee by the Human Capital team. The Human Capital Team shall advise all affected Employees of this policy. Willful withholding of information regarding a prohibited relationship/reporting arrangement will be subject to corrective action, up to and including termination. If a prohibited relationship exists or develops between two Employees, the Employee in the senior position must bring this to the attention of his/her supervisor/Human Capital team.

The Company retains the prerogative to separate the individuals at the earliest possible time, either by reassignment or by termination, if necessary.

(v) Other Situations

Because other conflicts of interest may arise, it would be impractical to attempt to list all possible situations. If a proposed transaction or situation raises any questions or doubts in an employee's mind, they should consult the Legal team and the Human Capital Team.

4.2.3. Protection of Interest

If an employee conceives or develops any new or advanced methods of improving process/formulae/ systems in relation to the operation of the company, such developments will need to be fully communicated to the company and shall remain sole right/property of the company. All company Non-Disclosure Agreements (NDAs) would remain applicable even after the date of separation of the employee.

4.2.4. Inducements

Employees will not offer or accept gifts, hospitality or other inducements which influence a decision, or engage in any form of bribery. We expect employees to report any such incident that they may be witness to.

4.2.5. Bribery

At Fractal, one of our foremost values is "Client First" and we value our client relationships. We acknowledge that building these connections may involve social activities like meals, or entertainment activities. However, we strictly prohibit the payment or receipt of gifts or bribes including in kind to gain business or financial advantage. Employees must avoid any actions that could suggest the Company is being improperly influenced. Bribes, defined as anything of value intended to secure an unfair advantage or given with an intention to exert inappropriate influence, are forbidden, regardless of their commercial value or source (funded through Fractal or through any individual employee). Even offering such items or gestures can violate legal standards, regardless of whether they are accepted or result in a benefit for Fractal. Maintaining integrity and transparency in all interactions is crucial to preserving the trust and ethical standards of our organization.

4.2.6. Gifts and hospitality

It might be customary, at times, to give or exchange unsolicited gifts during the traditional festive seasons or during certain corporate events. These should be restricted to promotional or advertising material or such items that are

customary or considered to be prudent or of a symbolic nature by the management, having regard to the nature of the business, the type of markets in which the Company is operating, and the event being observed. As per the anti-corruption laws, it would be illegal and unethical to give any gifts with intent to derive any benefit in return or could be perceived as a benefit derived in exchange of the gift.

In all countries, employees are required to report any gifts or hospitality exceeding USD 100 in value within a financial year to their line manager. If there is any uncertainty regarding the appropriateness or value of a gift or hospitality, employees should promptly consult their line manager for guidance. This practice ensures transparency and adherence to our ethical standards across all locations. For more details please refer to anti bribery ant-corruption policy (ABAC policy) on Employee Handbook.

4.2.7. Suspected Fraudulent behaviour

Any acts of commission or omission that adversely affect the company's business, such as bribery, fraud, pilferage, theft, and similar misconduct, are strictly prohibited. Any suspected fraudulent or unethical behaviour will be subject to a thorough investigation. Employees found to be involved in such activities may face disciplinary actions, including possible termination of employment, in accordance with the company's policies and procedures.

4.2.8. Communication

Employees will be truthful, helpful and accurate in their communication. Effective communication is vital to avoid misrepresentations, misstatements, misleading impressions and untruths. All communication material shall be prepared in alignment with this sentiment and should be adequately backed by documentation to support any claims or statements made. Information posted on the Company's website(s) shall be governed by the same standards as are applicable to other communication material.

We shall, on a timely basis, provide reliable and meaningful information about our products, services, operating results and other activities to legitimately interested persons and as may be required by law, subject to considerations of the legal requirements, cost and confidentiality.

Given the sensitivities involved, certain designated persons or groups of persons will be authorized to communicate on specified matters especially to the media, and no other person would be expected to communicate in an out-of-turn manner on those matters. We will maintain communication with our employees through our internal communication systems and by the consultative process.

4.2.8.1 Social Media

"Social Media" is the term given to websites and online tools that allow users to interact with each other via the internet by sharing information, opinions, knowledge, and interests. They can participate in social networks and online communities using sound judgment and common sense; however, they are obligated to protect personal, confidential and proprietary information belonging to the company, our clients or third parties with whom the company conducts business. Company e-mail addresses should not be used for employee's personal social media interactions. For more details please refer to Social Media Policy on Employee Handbook.

4.2.9. Maintaining Confidentiality of Information

We will protect the confidentiality of company, employee and client information. Revealing confidential company information could undermine Fractal's competitive advantage. Be aware of Fractal's security classification system.

Confidential information includes:

- Any information that the employee creates, receives, uses (in any form) or learns during their employment and/or affiliation with Fractal
- Any information that is not generally known by the public, our affiliates, or clients

- Any information of a sensitive nature that if disclosed, could result in financial or reputational harm to our clients or the company

Remember to be very careful when discussing confidential Fractal business and client business in public places and be sure of who employees are speaking to before disclosing information that might be commercially sensitive. Disclosure of information should only be made to the extent necessary to achieve our commercial goals. Remember to treat e-mail with the same professionalism and confidentiality as other more 'traditional' forms of communication, emails can have legal consequences too. Please refer to Data Classification Policy for more details

4.2.9.1 Data Privacy and Data Protection

Fractal respects the privacy of all data subjects and is committed to protect their rights.

Please refer to the Privacy and Data Protection Manual for more details, which is based on universally recognized frameworks and is in compliance with applicable laws and regulations across various geographies in which organization should be subject to regulation.

4.2.9.2 Information Security Guidelines for Data & Asset usage

All employees, contractors, interns, vendors, and other individuals working at or with Fractal Analytics must comply with the Information security guidelines. The below section is an indicative list and is not exhaustive in nature. It includes the different kinds of IT security violations and clarifies what constitutes violation of these protocols code of conduct and the stipulations on breaching of the conducts. Below is the list for code of conduct. The list includes, but is not limited to the following:

Unauthorized access to any system: Gaining unauthorized access to any of the Fractal's assets which includes IT systems, Physical infrastructure can lead to Financial / Reputational / Legal and / or Operational loss to Fractal. Any employee at Fractal trying to access other Fractal employee's IT system which includes but not limited to Desktops, Laptops, Networking devices, Servers etc. without prior approval from the CISO, from inside or outside of the Fractal's office shall face disciplinary actions as outlined in misconduct policy.

Attempts to hack the Fractal's IT infrastructure: Any employee trying to hack the Fractal's IT system including but not limited to Fractal's Laptops Desktops, Server, Networking Devices in or outside of the Fractal's office shall face disciplinary actions as outlined in misconduct policy.

Breaching of confidentiality agreement: Confidentiality agreement is signed between all the employees at Fractal and the organization itself. Any employee at Fractal found guilty of breaching the signed confidentiality agreement shall face disciplinary actions as outlined in misconduct policy.

Change Management Procedure not followed: Change management procedure is made to ensure that any changes made to Fractal's asset is tracked and approved. Any employee at Fractal not following the entire change management procedure for changes in any of the Fractal's IT systems which stores and / or processes confidential information shall face disciplinary actions as outlined in misconduct policy.

Clear Screen & Clear Desk Policy not followed: Users should keep sensitive or critical business information, e.g. on paper or on electronic storage media locked (ideally in a safe cabinet or other form when not required) especially when the office is vacated. Users should keep the system logged off when left unattended. Users not following this policy shall face disciplinary actions as outlined in misconduct policy.

Desktops, Laptops, networking devices not following hardening guidelines & checklist: Hardening guidelines are set by the organization to ensure security of IT systems. Any employees not following the hardening guidelines and checklist for Fractal's IT system shall face disciplinary actions as outlined in misconduct policy.

Obstructing the investigation process during and/or after an incident: Any employee trying to obstruct (which includes but not limited to modification, deletion, creation or destruction of evidence) the investigation, in case of any incident shall face disciplinary actions as outlined in misconduct policy.

Reporting of Information Security event / incident: Any employee who was found witnessing the information security incident and / or event but not reporting the same shall face disciplinary actions as outlined in misconduct policy.

Manipulation with video cameras and / or media storing recordings of video camera: Video camera, assists in achieving physical security for Fractal. Any employee at Fractal manipulating, destructing, alternating the video camera and / or its recording shall face disciplinary actions as outlined in misconduct policy.

Misplacing / Loss / Theft of Fractal's Laptop: All Laptop's and the information stored in that laptop, which are assigned to employees of Fractal, is the property of Fractal. Any employee found Misplacing / Loosing / Stealing the Fractal's property shall face disciplinary actions as outlined in misconduct policy.

Misusing of Fractal's email ID and / or sharing Fractal's email ID with anyone other than the respective clients: Fractal's email ID is Fractal's property. Any employee misusing its email ID for any unauthorized, prohibited, illegal activities, for personal advertisements, for registration on any websites without proper approval and / or by sending spams, shall face disciplinary actions as outlined in misconduct policy.

Multiple unauthorized access attempts to access Server Rooms: Server Rooms in Fractal contains critical IT Infrastructure. Access to Server Room is restricted only to designated members. Any employee, other than the designated members trying to gain unauthorized access by attempting multiple times by any means, shall face disciplinary actions as outlined in misconduct policy.

No participation in awareness or training programs pertaining to information security: Employees working in Fractal should be aware of the information security policies and procedures. Employees not participating in the awareness sessions and / or trainings shall face disciplinary actions as outlined in misconduct policy.

Password guidelines not followed. Easily guessable passwords used for login: All the Fractal's systems (Laptops, Desktops, Server, and Networking Devices) are to be password protected as it contains confidential information. Password guidelines are established to prevent it from unauthorized users. Employees working in Fractal should be aware of the Password protection policy and follow the guidelines to protect the systems from hackers, malicious users. Employees not following password guidelines shall face disciplinary actions as outlined in misconduct policy.

Practicing Shoulder Surfing: Shoulder surfing is one of the many social engineering techniques where a malicious user stands behind or sits beside the victim to gain confidential information without the knowledge of the victim. Any employee at Fractal found practicing Shoulder Surfing shall face disciplinary actions as outlined in misconduct policy.

Multiple unauthorized access attempts to access secure areas: Secure areas at Fractal are accessible only to authorized personnel. Any unauthorized employee / user found accessing or trying to access secure areas shall disciplinary actions as outlined in misconduct policy.

Sharing of Confidential information: Client information is very confidential in nature and cannot be shared with any unauthorized personnel via emails, verbal conversation or any other medium for communication without prior approval from Reporting Manager. Any employee found breaching the confidentiality of information and sharing the confidential information with unauthorized users shall face disciplinary actions as outlined in misconduct policy.

Password Sharing: Passwords is one of the most commonly used method by all users for protection of Fractal's IT assets which includes but are not limited to desktops, laptops, networking devices, servers etc. Sharing of these passwords which protect Fractal's IT assets may lead to unauthorized access to Fractal's confidential information. Any employee found sharing passwords of Fractal's IT assets shall face disciplinary actions as outlined in misconduct policy.

Storage devices left unattended: Storage devices which include but are not limited to CD's, DVD's, External Hard Disk or any devices which can store data might contain confidential information or might even contain malicious data to corrupt the Fractal's information. Leaving such devices unattended keeps confidentiality of Fractal's information at risk. Any employee found leaving such storage devices unattended shall face disciplinary actions as outlined in misconduct policy.

Unauthorized storage of confidential information on storage devices: Storing of confidential information on storage devices without prior approval breaches the confidentiality of the information. Storage devices which include but are not limited to CD's, DVD's, External Hard Disk or any devices which stores data can be used on Fractal's assets and property only with prior approval from reporting manager. Any employee found storing confidential information without prior approval shall face disciplinary actions as outlined in misconduct policy.

Storage of confidential information without encryption or password: Storing of confidential information on your Fractal's Laptops, Desktops, Networking devices, Servers or on any storage devices without password protection leaves it open to risk of breaching confidentiality. Any employee not storing such files with password, or any other encryption method shall face disciplinary actions as outlined in misconduct policy.

Passwords not stored securely: Storing of passwords which are used for locking Fractal's IT systems, on paper and / or in areas accessible to other employees makes the Fractal's IT systems vulnerable to unauthorized access. Any user not storing the passwords securely shall face disciplinary actions as outlined in misconduct policy.

Theft of Fractal Assets: Fractal's assets are property of Fractal only. Any employee found stealing Fractal's Assets which includes but not limited to IT Assets, Infrastructure, Documents etc. shall face disciplinary actions as outlined in misconduct policy.

Unauthorized alterations to Fractal's copyright material: Any employee found modifying, deleting, copying Fractal's copyright material shall face disciplinary actions as outlined in misconduct policy.

Unauthorized usage of social networking websites: Usage of social networking websites which include but not limited to Facebook, Twitter etc is restricted on Citrix environment. Any User found violating the conduct shall face disciplinary actions as outlined in misconduct policy.

Tailgating in Secure areas: Tailgating in secure working areas is not authorized. Any employee found tail gaiting in secure working areas shall face disciplinary actions as outlined in misconduct policy.

Unauthorized recording: Usage of any unauthorized photographic, video, audio, any media and / or electronic equipment in secure working areas is strictly prohibited. Any employee found breaching this conduct shall face disciplinary actions as outlined in misconduct policy.

Usage of generic User ID's: Generic user ID's like admin, root, user, administrator is easily hackable by guessing or by Brute Force method which is commonly used by hackers. Any employee found using generic User ID on any of the Fractal's IT system shall face disciplinary actions as outlined in misconduct policy.

Usage of Personal Computing devices: Any Personal computing devices which includes but not limited to Laptops, Desktops, I-Pad, Tab etc shall not be used on Fractal's property without prior approval. Also, usage of personal computing devices for accessing information of Fractal's clients, outside Fractal office requires approval. Any employee breaching the conduct shall face disciplinary actions as outlined in misconduct policy.

Usage of Personal email ID's: All users at Fractal are assigned with Fractal's email ID. This email ID is used for communication with clients. Any communication with client and sharing of any confidential information needs to be done through Fractal's email ID. Personal email ID can be used in an emergency with approval from the reporting manager. Any employee found using personal email ID's which include but not limited to Google, Yahoo, Hotmail etc without approval shall face disciplinary actions as outlined in misconduct policy.

Usage of Pirated Software products: Usage of pirated products can introduce the IT system to Virus, Malware and other kinds of threats. Using pirated software products on Fractal's IT systems is strictly prohibited. Any employee violating this conduct shall face disciplinary actions as outlined in misconduct policy.

Usage of removable devices: Usage of removable devices which includes but not limited to USB's, CD / DVD's, External Hard Disk etc can cause harm to Fractal's IT systems. Any user using removable media in Fractal's IT system without prior approval shall face disciplinary actions as outlined in misconduct policy

Usage of websites: Any user using/Attempting to access obscene, restricted, malicious, violence material, sexual exploitation websites shall face disciplinary actions as outlined in misconduct policy

Write access on external media: Employees Gaining or trying to gain write access on external devices which include but not limited to CD's / DVD's, USB, Bluetooth without prior approval can be interpreted as attempt to gain unauthorized access to Fractal's assets and shall face disciplinary actions as outlined in misconduct policy.

4.3. Protection of Company Assets

Employees should protect our brand, physical, financial and intellectual assets. Employees are responsible as individuals for the security and protection of the assets used in their job. This includes the proper accounting for the use of any company resources. For more details refer Fractal's Policy on IT Security Policy.

One of our most valuable assets is the Fractal brand and its reputation. A strong brand is essential for sustainable success, especially in fast-changing and highly competitive markets. Fractal's brand must be protected with as much care as our buildings or equipment. Products, services or marketing communications that are not consistent with the meaning of the brand, bad press publicity, or improper use of the logo undermine our brand and competitiveness.

4.3.1. Intellectual property

Company property includes Intellectual Property rights such as Patents, Trademarks, copyrights, designs, strategies, plans, trade secrets and similar items that are not in the public domain – should be used only in the course of and for Company business, with proper care and safeguards.

The information, ideas, concepts and 'know how' described, documented or contained in the company's communications systems and related databases are the intellectual property of the company. Anything conceived or produced by the employee in connection with your tenure at Fractal – including documents, reports, software, ideas, processes, methodologies and "know-how" – is the intellectual property of the company.

The copying or use of the company's intellectual property for personal use and/or the benefit of any other third party during or after employment with the company is prohibited.

4.4. Inclusive, Respectful and Safe Workplace

4.4.1. Inclusion, mutual trust and respect

At Fractal, we are committed to fostering an environment characterized by fairness, openness, and mutual respect. We aim to create a working culture that is inclusive and empowering, enabling every employee to make meaningful

contributions. This commitment extends to our interactions with suppliers, business partners, and customers. Managers are expected to lead by example, demonstrating fairness and discouraging prejudice.

Fractal's people principles outline some of the basic requirements regarding expected from people working with us. Any disrespectful behaviour and harassment, including verbal and non-verbal actions, written communications, and social media interactions, are not tolerated. We evaluate behaviour based on its impact on the recipient and expect all employees to treat others with dignity and professional courtesy.

4.4.1.1 Non Retaliation Policy

Fractal is committed to upholding the highest ethical standards and fostering a workplace free from inappropriate or unlawful behaviour. Employees, former employees, agents, and third parties are encouraged to report any concerns regarding any unethical, fraudulent, or illegal behaviour or any other suspected violations of the Company's Code of Conduct, policies, or applicable laws without fear of retaliation. Employees are expected to report any instances that can be qualified as harassment, discrimination, retaliation or workplace violence or threats, even if the behaviour has stopped occurring. Adverse action will not be taken against individuals who report or assist in the investigation of such concerns, provided the reports are made in good faith. Confidentiality will be maintained to the extent possible. All allegations of retaliation will be thoroughly investigated, and appropriate disciplinary measures, including termination, will be implemented if necessary. Potential legal violations must be directed to the Legal team. All concerns will be addressed confidentially (to the extent possible) and with urgency, post evaluating the nature and severity of the incident.

4.4.1.2 Harassment

We do not tolerate harassment or unfair discrimination in our working environments. It means being committed to ensuring that our people work in a workplace that sets them up for success and is free of discrimination on the basis of gender, race, age, religion, sexual orientation or disability, and free from harassment – any conduct, comment, gesture, graphic or contact that is likely to cause offence or humiliation. It means that any act that makes people feel unsafe will not be tolerated.

4.4.1.3 Prevention of Sexual Harassment

Fractal strictly prohibits any kind of sexual harassment. Sexual harassment is defined as unwelcome sexually determined behaviour (whether directly or by implication) including but not limited to:

- Physical contact and advances
- A demand for request for sexual favours
- Sexually coloured remarks
- Showing pornography or
- Any other unwelcome physical, verbal or non-verbal conduct of sexual nature or bullying
- Any conduct that may reasonably be interpreted as harassment, whether such conduct is pervasive / severe enough to meet the above requirements of harassment.
- It is important to note that the actual or perceived impact of a behaviour on the recipient rather than the intent of the offender, determines whether the behaviour constitutes sexual harassment.

This policy is in accordance with the applicable provisions in the jurisdiction of the locations where Fractal operates, for example in India, The Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013 requires an employer to set up an 'Internal Committee' ("IC") at each office location, to hear and redress grievances pertaining to sexual harassment of women.

For more details, please refer to Fractal's Policy on Prevention of Sexual Harassment at Workplace.

4.4.2. Equal Employment Opportunity

Fractal is an "equal opportunity" organization that prohibits discrimination or harassment based on race, color, religion, national origin, sex, age, sexual orientation, marital status, citizenship status, or disability. Our hiring and employment practices are designed to ensure fairness and inclusivity.

4.4.3. Health and Safety

Fractal is committed to maintaining the health and safety of our employees and ensuring that our business practices do not adversely affect the well-being of anyone involved. We take proactive steps to protect our workforce and others impacted by our operations, products, and services. See **(Health and Safety Policy)**

4.4.4. Slavery and Human Trafficking

Fractal is committed to conducting its business with integrity, honesty, and to high ethical standards. We abhor all forms of slavery and human trafficking and fully support measures to ensure that abusive labour practices are eradicated. Fractal is committed to ensuring that our business practices are free from abusive labour practices, ands aligns with our commitment to integrity in all business relationships. We are committed to ensuring that there is no modern slavery or human trafficking in any part of our business. Our Code of Conduct reflects our undertaking to act lawfully and with integrity in all our business relationships and reinforce our efforts to ensure that slavery and human trafficking does not occur in any aspect of our business.

4.4.5. Under-age employment or Child Labor

Child labour is defined as employing any person younger than the minimum age allowed by law in the jurisdiction in question.in no event will we knowingly employ anyone younger than eighteen (18) years of age or as applicable as per law.

4.4.6. Employee Grievance Redressal Mechanism

Fractal recognizes that engaging in a formal grievance procedure can be a challenging and emotional experience for all parties involved hence Fractal ensures a fair and standardized approach to addressing employees grievances. Employee grievances may cover various workplace aspects but, for this process, are limited to Human Capital (HC)-related issues such as workplace disputes, compensation, policy violations, discrimination, and career development concerns. Employees are required to communicate their grievance in writing to HC Business Partner and additionally can also raise a ticket on HC Helpdesk Portal
- https://hchelpdesk.fractal.ai/app/hchelpdesk/HomePage.do.

4.5. Code of Conduct Awareness, education, and training

- All employees of the organization and contractor should receive appropriate awareness education and training and regularly updated on organization policies and procedure, as relevant to their job functions.
- Awareness training can use different delivery media including classroom based, web based. All employees should read the Code and understand the same thoroughly.
- In the event of changes to the Code, same should be conveyed to all concerned employees and temporary workers / contractors by either or all of the following.
    - Sending mails related to concerned employees.

- Displaying changes on notice boards / bulletin board.
- Displaying security awareness posters on user's desktops.

- If required training session should be conducted.
- Awareness programs should be conducted on a regular basis or in the event of major changes.
- Every new joiner should go through the Code of Conduct training within two months of joining Fractal or going live on operations floor whichever is earlier. An annual refresher course should be conducted for all employees educating them on various aspects of the Code.

4.6. Disciplinary Process

The following paragraphs deal with the disciplinary procedures, which could be used as indicative guidance for the Company constituents while formulating their respective disciplinary procedures.
Depending upon the nature and seriousness of non-compliant behaviour/violation of the Code, the Company may take corrective action against the erring employees in accordance with the misconduct policy. Apart from recovery of full / partial monetary loss caused to the Company by the employee's behaviour, the Company may prefer civil or criminal action against errant employees. Such actions may include penalties as deemed appropriate considering the nature of violation and its implication on the Company. The extenuating / mitigating circumstances, if any, may also be considered while taking action.

These actions could be:

- Verbal warning or reprimand
- Warning letter in writing
- Adversely impacting annual performance rating
- Withholding of increment
- Withholding of performance linked bonus / incentive (partly or completely)
- Withholding of promotion
- Termination of services

A formal disciplinary process will be initiated on employees who have violated the Code of Conduct. Management will collect as much documentary evidential information as required before proceeding with disciplinary action. The HCBP and the relevant Business Unit should be notified and will actively involved in all disciplinary actions and if required Legal counsels should be sought.

5. Responsibility to uphold the Code of Conduct

Each employee has a responsibility to identify and report in good faith any potential or actual violations of the Code of Conduct or related concerns through consultation and/or reporting. If one becomes aware of a potential unethical, illegal or fraudulent action, or other violation of company policy, whether committed by a colleague, client, supplier, contractor or other individual or organization associated with the company, it is important that the employee reports the circumstances through an appropriate reporting channel.

The Code cannot provide definitive answers to all questions. For that we must ultimately rely on each person's good judgment of what is required to adhere to the company's highest standards, including a sense of when it is proper to seek guidance on the appropriate course of action. If you have questions or if you are in doubt about the best course of action in a particular situation, please seek guidance as described below:

- Your Manager - Speak with your manager or a member of your leadership team to discuss concerns or if you have questions.

- Human Capital Business Partner (HCBP) - Your local HCBP representative is another valuable resource for advice and counsel.
- Legal Team - For any compliance questions or to obtain advice/assistance with the interpretation of laws, regulations or policies.

Necessary disciplinary action will be taken against any employee not following the policies and procedures laid down by the Fractal. Similarly, action will be taken against those employees encouraging/observing such an activity and not reporting the same to the concerned authority. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as per Fractal policies.

6. Special situations and exceptions

Fractal's top management, Human Capital team, Indian government, or any other regulatory body or bodies norms overrides Fractal's Code of Conduct at a particular point in time.

7. Enforcement

Necessary disciplinary action will be taken against any employee not following the policies and procedures laid down by the Fractal. Similarly, action will be taken against those employees encouraging/observing such an activity and not reporting the same to the concerned authority. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as per Fractal HC and Code of Conduct policies.

8. Review And Updates:

At Fractal, we recognize the importance of maintaining up-to-date policies to ensure compliance with laws, regulations, industry standards, and to meet the evolving needs of our company. Human Capital Team shall be responsible for reviewing this policy annually or as deemed necessary. Upon any updates and changes to the policy, Human Capital Team will shall ensure timely communication to all employees, candidates, and relevant stakeholders.

9. Definition and Acronyms

Definitions

Term	Explanation
Employee	Person hired to perform a job or service for Fractal, and one who is directly employed or hired on a contractual basis
Client	All the clients of the organization who avail services or products provided by the Fractal
Vendors	All third parties which includes, but is not limited to vendors, volunteers, contractors, consultants, temporaries, interns and others who have access to, support, administer, manage, or maintain Fractal's information or physical assets

Acronyms

Acronym	Full Name
Fractal/ Company / Fractal Analytics	Fractal Analytics Limited
HCBP	Human Capital Business Partner
Code	Code of Conduct