Code of Business Conduct and Ethics

To All Directors, Officers, Employees and Temporary Workers of Pipeline Infrastructure Limited, EnCap Investment Manager Private Limited and Pipeline* Management Services Pvt. Ltd.*,

The Code of Business Conduct and Ethics (the "Code") applies to all directors, officers, employees and Temporary employees of Pipeline Infrastructure Limited, ***EnCap Investment Manager Private Limited a***nd Pipeline Management Services Pvt. Ltd. (collectively, "PIL", "we," "us," "our" or the "company")

It has always been and remains our policy that all of our activities should be conducted with the utmost honesty and integrity and in full compliance with all legal and regulatory requirements. In varying degrees, as a manager or employee of the company, you represent us in your dealings with others, whether they be other employees, customers, suppliers, competitors, governments or the general public. Each of us is responsible for preserving and enhancing the company's world-class reputation and the Code sets out what is expected of all of us who are part of the team.

The enclosed Code, which has been endorsed by PIL's Board of Directors, sets out the commitments we all must make as part of the PIL's team. We urge you to read it carefully.

The Code does not cover every situation you may encounter while at PIL and that is not its purpose. Rather the Code sets forth basic principles and standards to which you must adhere. When in doubt, please refer any questions to your supervisor or Head – Risk (or the Chair of the Board in the case of directors).

Thank you for your continued dedication to PIL and for your commitment to upholding the standards set forth in the Code.

Yours truly,

Arun Balakrishnan
Chairman
Pipeline Infrastructure Limited

Akhil Mehrotra
Managing Director
Pipeline Infrastructure Limited

Code of Business Conduct and Ethics

The contents of this Code are the property of the PIL and both, its use and dissemination, are for internal purposes only. This document may not be reproduced, stored or distributed, in any format or by any means, whether electronic or physical, without the prior formal authorization of the Company.

SUMMARY OF THE CODE'S PRINCIPLES[1]

PROTECTING THE COMPANY'S ASSETS, RESOURCES AND DATA

- We often have sensitive confidential information about PIL, other companies, our parent company and investors, our customers, and our directors, officers employees, Temporary worker and Off-roll employees; preserving the integrity of this information is vital to our business and reputation and is necessary to meet our obligations under data protection laws.
- Electronic communications relating to business activities may not be conducted through electronic communication systems that have not been specifically approved for business activities, including (among others) personal email accounts, personal text messaging, non- approved chat forums or AI tools, and social media.
- Personnel other than independent directors must complete mandatory data protection training and mitigate cybersecurity risks by being vigilant about opening attachments or clicking on links.

ACCURACY OF BOOKS AND RECORDS AND PUBLIC DISCLOSURES

- We should take care that our books and records are accurate and that all of our business transactions are properly authorized.
- Because our parent companies are public companies, we must ensure that our communications and other disclosures to the market are true and accurate.

DUTIES TO STAKEHOLDERS

- A company's reputation is Critical, and we should act responsibly in dealings with our customers, clients, suppliers, investors, other stakeholders and competitors.

COMMUNICATIONS AND MEDIA

- In this digital era, be careful in your written communications made over company information systems, such as email and messaging applications, as this is a permanent record.
- You must ensure that your online activities, including your use of online social media, are appropriate and reflect well on PIL.

CONFLICTS OF INTEREST AND PERSONAL BEHAVIOUR

- As a representative of the company your personal behavior must be consistent with our values.
- We must be cognizant that we face a heightened risk that one's personal interests may conflict with or appear to conflict with the interests of the company.

POSITIVE WORK ENVIRONMENT

- We value diversity, equity and inclusion, we should all do our part to create a respectful work environment where everyone feels safe and productive.
- Our success is dependent on establishing a workplace culture free from discrimination, violence, harassment and other negative influences.

COMPLIANCE WITH LAWS, RULES, REGULATIONS AND POLICIES

- We, including our partner company, operate in many jurisdictions and are subject to different laws, rules and regulations; you need to be aware of the laws that apply to your activities so that you can comply with them; ignorance of the law is no excuse.
- The company has corporate policies that you must be familiar with, as they govern your business practices and other conduct while at PIL.

1. These principles are for summary purposes only. For more detailed information on each of these items consult the Code attached.

FREQUENTLY ASKED QUESTIONS

WHY DO WE HAVE A CODE?

The Code serves as a guide for how you should conduct yourself as a member of the PIL team. Preserving our corporate culture and ensuring compliance with legal, regulatory and fiduciary duties is vital to the organization and following the Code helps us do that.

WHO MUST FOLLOW THE CODE?

The Code applies to the company and all of its managed operations. It thereby applies to all directors, officers, temporary workers and employees of the company regardless of their location.

WHAT ARE YOUR RESPONSIBILITIES?

You have two responsibilities. First, you must follow every aspect of the Code and the policies referred to herein and certify your commitment each year. Second, if you suspect someone may be violating the Code or the policies referred to herein, you have an obligation to report it. To make a report, follow the section of the Code: "Reporting Potential Code Violations".

HOW WILL I KNOW IF THERE IS A PROBLEM?

The Code attempts to deal with the most common issues that you may encounter, but it cannot address every question that may arise. When you're not sure what to do, ask yourself the following questions:

- Is it illegal?
- Does it feel like the wrong thing to do?
- Would you feel uncomfortable if others knew about it?
- Will it have the potential to create a negative perception of you or the company?
- Do you have a personal interest that has the potential to conflict with the company's interest?

If you answer "yes" to any of these questions your proposed conduct may violate the Code and you should ask for guidance.

HOW SHOULD I ASK FOR GUIDANCE?

If you have questions about the Code, any policy or guideline referred to herein, or about the best course of action to take in a particular situation, you should seek guidance from your supervisor /Head – Risk.

WHAT IF I WOULD LIKE TO MAKE AN ANONYMOUS REPORT?

You may make an anonymous report by contacting the company's reporting hotline, which is operated by an independent third party and is available 24 hours a day, 7 days a week. If you choose to make an anonymous report, your anonymity will be protected to the fullest extent possible as permitted by law. Keep in mind, however, that maintaining your anonymity may limit the company's ability to investigate your concerns.

WHAT ARE THE CONSEQUENCES FOR VIOLATING THE CODE?

Violations of the Code or the policies and guidelines incorporated by reference herein, can vary in its consequences. If you're an employee, it could result in a reprimand or other disciplinary action, including the termination of your employment for cause. If you're a director, a violation may necessitate your resignation or termination under the terms of your director's agreement, if any. Certain violations of the Code also contravene applicable laws and therefore can have severe consequences outside of PIL. Depending on your actions, failing to comply with the Code could lead to civil or criminal prosecution, which could result in substantial fines, penalties and/or imprisonment.

TABLE OF CONTENTS

INTRODUCTION **6**
PROTECTING THE COMPANY'S ASSETS, RESOURCES AND DATA **6**
ACCURACY OF BOOKS AND RECORDS AND PUBLIC DISCLOSURES **9**
DUTIES TO STAKEHOLDERS **10**
COMMUNICATIONS AND MEDIA **10**
CONFLICTS OF INTEREST AND PERSONAL BEHAVIOUR **11**
POSITIVE WORK ENVIRONMENT **12**
SUSTAINABILITY MANAGEMENT **13**
HUMAN RIGHTS AND Anti-MODERN SLAVERY **14**
COMPLIANCE WITH LAWS, RULES, REGULATIONS AND POLICIES **15**
REPORTING POTENTIAL CODE VIOLATIONS **17**
DISCIPLINARY ACTION FOR CODE VIOLATIONS **18**
STATEMENT OF COMPLIANCE **18**
WAIVERS **19**
AMENDMENTS **19**
CONTACT INFORMATION **19**
LEGAL NOTICE **20**
SCHEDULE A **21**

INTRODUCTION

This Code of Business Conduct and Ethics (the "Code") applies to all directors, officers, employees and temporary workers[2] (collectively, "you") of Pipeline Infrastructure Limited, EnCap Investment Manager Private Limited and Pipeline Management Services Pvt. Ltd. (PMSPL, EnCap, collectively, "PIL", "we," "us," "our" or the "company")

STANDARDS OF BUSINESS CONDUCT

PIL seeks to foster and maintain a reputation for honesty, openness, trust, integrity, and professionalism. The confidence and trust placed in PIL by our stakeholders is something we value greatly and endeavor to protect. In many respects, our reputation is our most vital business asset. Accordingly, all our activities should be conducted with honesty and integrity and in compliance with applicable legal and regulatory requirements.

We have adopted the Code and related policies and procedures to preserve our culture and to ensure compliance with legal, regulatory and fiduciary requirements applicable to our activities. We expect and require that you meet the letter and spirit of the Code (and related policies and procedures - as updated and/or superseded from time to time). This code incorporates by reference the following corporate policies and programs which should be read in conjunction with the Code:

- Anti - Bribery and Corruption Policy
- Whistle-Blower Policy
- Interaction with Public Officials Policy
- Gifts, Entertainment and Hospitality Policy
- Third Party Management Policy
- Information Security Policy
- CSR Policy
- Positive Work Environment
- Anti-Modern Slavery and Human Trafficking Policy

PROTECTING THE COMPANY'S ASSETS, RESOURCES AND DATA

The company's assets are to be used for legitimate business purposes only.

The company's assets are for business use, not personal use. The company's assets span many categories. Assets can be physical, tangible goods, such as office supplies, furniture, computers or intangible items, such as emails, intellectual property or data. You have a responsibility to safeguard the company's assets from loss, damage, theft, misuse and waste. If you become aware of loss, damage, theft, misuse or waste of our assets, or have any questions about your proper use of them, you should speak with your supervisor. The company's name (including its corporate letterhead and logo), facilities and relationships are valuable assets and must only be used for authorized company business.

If you use the company's assets for personal benefit, or are otherwise wasteful with the company's assets, you may be in breach of your duty to the company. You have a responsibility not to abuse company resources for reimbursement. Any requests for reimbursement for authorized company expenses must be for legitimate business expenses. If you are unsure whether a certain expense is legitimate, you should speak with your supervisor or Head – Risk. Refer Employees reimbursement claim policy.

Confidential information must be protected at all times.

We must protect confidential information in our possession. This includes information about us and information about our customers, suppliers, parent company and other third parties. Confidential information includes, but is not limited to, material non-public information, all confidential memos, notes, lists, records and other documents in your possession, in hard and soft copy. All of these are to be delivered to the company promptly after your employment ceases or at any time upon the company's request, and your obligation to protect this information continues after you leave the company. You must protect hard and soft copies of confidential information that are removed from the office (e.g., to be worked with at home or at external meetings).

It is important to use discretion when discussing company business. This includes respecting information barrier protocols where such protocols exist and not discussing company business with those individuals at the company that have a "need to know" the information. Additionally, be careful not to discuss company business in public places such as elevators, restaurants, and public transportation, or when using your phone or email outside of the office. You should also be careful not to leave confidential information in unattended conference rooms or in public places where others can access it. You must complete mandatory data protection training and mitigate cybersecurity risks by being vigilant about opening attachments or clicking on links.

We place high importance on combatting cybersecurity risk and, as such, conduct phishing simulations on a regular basis. The company employs disciplinary protocols related to failures of its simulations, which are implemented at company's discretion. These protocols include penalties and other measures that escalate in severity for successive failures. These measures may include any or all of the following: informing your manager of the infraction; assigning of mandatory additional cybersecurity training (both live and online); written reprimands; reduction or elimination of your annual bonus and/or other discretionary awards; and/or termination of your employment.

Please refer to the Data Protection Program for further information about how to protect confidential and personal data. While at PIL, if you become aware of confidential information about the company or another entity that you know or suspect has been inadvertently disclosed, seek guidance from Head – Risk before using or acting upon this information.

Personal data[3] held by or on behalf of the company must be used in compliance with applicable data protection laws. The company collects, processes and transfers personal data regarding individuals both inside and outside the organization in accordance with the Data Governance Framework. This is necessary to effectively and efficiently administer and manage the operation of our business, including compliance with applicable laws. Personal data[3] includes, among other things, sensitive personal, medical, financial information and customer information. In general, personal data will only be held by the company for as long as we have a legitimate business need to retain it. We should take all reasonable steps to only hold personal data for as long as we have a need to retain it and in accordance with applicable law and company's Data Protection Program. For more information about compliance with data protection laws, refer to the related company policies.

Collection and use of personal data are subject to various legal and regulatory requirements. You must take all reasonable steps to ensure that personal data is kept confidential and accessed only by those individuals at the company that have a need to know this information to carry out their duties It may be necessary to disclose personal data to a third-party (e.g., so that a third-party may provide services to the

[3] "Personal data" has the meaning given to it or any similar term in applicable data protection or privacy legislation.

company or acquire an asset or business of the company) to the conduct of business; it must be ensured that such transfer complies with applicable legal and regulatory requirements. This may include ensuring the third party is subject to a written agreement which contains confidentiality obligations and, where relevant, other obligations which must be included under the applicable data protection laws. In all other cases, you may only disclose personal data pursuant to a legal or regulatory requirement. Personal data must be stored exclusively on approved technologies.

You are responsible for ensuring that you understand and comply with our *Data Governance Framework and Program*. For more information about compliance with data protection laws, refer to the related company policies

Intellectual property belongs to the company.

During the course of your employment, you may be involved in the creation, development or invention of intellectual property such as concepts, methods, processes, inventions, confidential information and trade secrets, know-how, physical products, ideas, plans, programs, software, applications, code, works of authorship, trademarks, service marks and designs, alone or jointly with others, including but not limited to the improvement of existing intellectual property belonging to the company. All such intellectual property and the rights therein shall be owned by the company and your moral rights to such intellectual property, if any will be waived. You are responsible for cooperating with the company and providing all necessary assistance, including the preparation and execution of any necessary documentation such as assignments and applications to register rights before relevant government authorities on behalf of the company, to ensure that all intellectual property and related rights become the exclusive property of the company.

The documents of the company must be preserved.

It is critical that you help preserve our business records, follow the guidelines set forth in any document retention policies and comply with related legal and regulatory requirements. If you are notified that your documents are relevant to an anticipated or pending litigation, investigation or audit, you must follow the guidance set forth in the notification you receive from legal counsel regarding retention of documents and act in accordance with company's *Record Retention Policy*.

Ensure Generative Artificial Intelligence (AI) Tools are used appropriately.

Generative AI tools such as ChatGPT, Co-Pilot, Claude Gemini (including Google Search), Bing, Ernie, and other products with pre -trained language models are powerful tools that can benefit our business if used appropriately. The use of certain tools, however, can present significant risks relating to the protection of confidential information (including personal data) and the reliability of your work and the company's decision-making that are based on AI generated outputs.

Higher risk AI tools, as defined in the AI Governance Policy, can only be used if they have been approved for the specific use in accordance with the procedure described therein. If you want to use a high-risk AI tool, you must submit an AI Approval Request Form and receive approval before using the AI tool. You can use AI tools that are not high-risk without approval, subject to applicable company policies. Confidential information should not be shared with, input into, uploaded to, or used to train AI tools unless such use has been approved in accordance with the [AI Usage Policy] or other applicable policies.

When using AI tools, you must carefully review and validate any AI-generated output for quality and accuracy. You must not rely on AI output to make important or significant business, HR, or legal decisions.

You must not integrate any AI tool - or any AI-generated output - into existing company IT processes where disruption could affect a company entity's ability to comply with legal or regulatory obligations or to provide critical services, unless you have obtained specific approval.

You are responsible for ensuring that you understand and comply with our restrictions on the use of AI tools, as set out in the IT/OT Unified Framework.

ACCURACY OF BOOKS AND RECORDS AND PUBLIC DISCLOSURES

Ensure that the books and records of the company are complete and accurate and that all business transactions are properly authorized.

The books and records of the company must reflect all its transactions in order to permit the preparation of accurate financial statements. Employees must never conceal information from (i) an external auditor;(ii) an internal auditor; (iii) an audit committee of the company. In addition, it is unlawful for any person to fraudulently influence, coerce, manipulate or mislead an external auditor of the company.

The company's contracts and agreements govern our business relationships. Because the laws governing contracts and agreements are numerous and complicated, we have put in place policies and procedures to ensure that any contract entered into by the company has the appropriate level of approval. As a result, employees who enter into contracts or agreements on behalf of the company must have proper authorization to do so and, prior to their execution, these documents must be reviewed by legal counsel where required by policy or practice. Consult a member of internal legal counsel if you are unsure whether a contract requires a review.

If you are unsure whether you have proper authorization to enter into a contract on behalf of the company, refer to the company's Delegation of Authority (DoA)/ Sub Delegation of Authority and thresholds therein.

Ensure that the company provides full, true and plain public disclosure.

All employees who are responsible for the preparation of the company's public disclosures, or who provide information as part of this process, must ensure that public disclosures of information are made honestly and accurately. Employees must be aware of and report any of the following: (a) fraud or deliberate errors in the preparation, maintenance, evaluation, review or audit of any financial statement or financial record; (b) deficiencies in, or non-compliance with, internal accounting controls;
(c) misrepresentations or false statements in any public disclosure document, such as annual and quarterly reports, prospectuses, information/proxy circulars and press releases; or (d) deviations from full, true and plain reporting of the company's financial condition.

Additionally, each person who is in a financial reporting oversight role, and their family members, are prohibited from obtaining any tax or other services from the external auditor, irrespective of whether the company or such person pays for the services.

DUTIES TO STAKEHOLDERS

Deal fairly with the company's stakeholders.

You must deal fairly with the company's customers, suppliers, other stakeholders and competitors. To preserve our reputation and relationship with stakeholders, do not engage in any illegal or unethical conduct when dealing with stakeholders or competitors.

COMMUNICATIONS AND MEDIA

Use the company's various forms of communication properly and appropriately.

All business matters communicated in writing must be via the company's email system and / or through other systems provided and approved by the company for such use in accordance with the ***Cyber Security Policy***. These systems must be installed by the PIL IT team on your devices and only company-managed versions of those systems are approved. You must always use our e-mail, Internet, telephones and other forms of communication appropriately and professionally. Employees must comply with our Information Security Policy and all related policies. While we appreciate the need for limited use of these tools for personal purposes, any such use should not be excessive or detract from your work.

Employees must not email business information to their personal email accounts or maintain a copy of business information on their personal computers, other non-company owned electronic devices or other non-approved external systems or applications. When using company-provided technologies such as computers, cell phones and voicemail, you should not expect that the information you send or receive is private. Your activity may be monitored to ensure these resources are used appropriately and are in compliance with the company's policies as well as applicable laws and regulations.

Employees should keep their company login ID and password (including multifactor authentication) secure and not share these credentials with anyone (internal or external). While using communication channels, employees must comply with PIL's Information Security Policy and all applicable policies. Personnel should take care when using the company's email system, other systems and devices to ensure that no viruses, malware or similar items are introduced into the systems or devices, including by clicking on links in phishing emails. Be cautious of social engineering tactics (including email, voice and text-based phishing) as they can manipulate your trust and compromise the security of our organization. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious. Always report all suspicious messages using the "**Report Message**" button in Microsoft Outlook. Promptly report any unusual or suspicious activity to the Cyber Security Team (***pil.cybersecurity@pipelineinfra.com).*** Your vigilance is crucial in ensuring the integrity of our systems, especially if you use our IT equipment/devices outside the workplace. Our system contains information which is confidential and subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy/Guideline.

Be cautious in your use of social media.

The company's social media policy is that, unless you are expressly authorized, you are strictly prohibited from commenting, or posting about, or otherwise discussing the company, its customers, Personnel as well as our parent company and its securities, investments and other business matters on all social media

forums, including, but not limited to, social networks, chat rooms, wikis, virtual worlds and blogs (collectively, "social media"). As a representative of the company while engaging in online activities ,you must ensure that your behavior online, including on social media, is appropriate and consistent with our values.

Do not speak on behalf of the company unless authorized to do so.

Because our parent company is a public company, it is important to ensure our communications to the investing public are: (a) timely; (b) full, true and plain; and (c) consistent and broadly disseminated in accordance with all applicable legal and regulatory requirements. You may not make public statements on the company's behalf or our parent company's unless you have been designated as a spokesperson under social media Policy.

Our parent company employs professionals who are trained and qualified as spokespersons to release information to the public and legal counsel who are authorized to communicate with regulators, stock exchanges, and other members of the public or media. You may be contacted by a member of the media, a shareholder, a financial analyst, a governmental authority or any other third party for information about the company or our parent company and its business, and a response can have far-reaching implications, including effects on our ability to compete. When we provide information on the company's operational strategies, financial results or other material information, we must ensure both that the information is accurate and that it is an appropriate time to "go public" with that information. If you receive a request from outside the company to speak on the company's behalf and you are not authorized to do so, refer the request to your supervisor, who may forward the request to the MD, who may seek the guidance of individuals at our parent company employed in investor relations or communications.

CONFLICTS OF INTEREST AND PERSONAL BEHAVIOUR

Exhibit personal behavior that reinforces a positive image of you and the company.

Your personal behavior, both inside and outside work, should reinforce a positive image of you, the company, its business activities, and its clients, and our parent company. It is essential to use good judgment in all your personal and business dealings. You should refrain from engaging in activities that could hurt the company's reputation, or yours, and that could undermine the relationship of trust between you and the company. Personnel who have acted inappropriately may be subject to disciplinary action up to and including termination for cause.

Remember your duties to PIL, when participating in outside personal interests; obtain permission before pursuing business activities outside the scope of your role within the company.

The company encourages Personnel to be active participants in their community. While pursuing personal, political, not-for-profit activities or other similar activities, be mindful that your participation in any outside interest must not prevent you from adequately discharging your duties to the company and should not conflict with or otherwise be averse to the company's interests. In addition, ensure that when you are involved in these activities you are not seen to be speaking or acting on behalf of the company or the parent company without express authority.

"Outside Business Activities," otherwise known as "OBAs" include any business activities outside the scope of one's role with the company, including any activity as an employee, independent contractor, sole proprietor, officer, director, or partner of another business organization, regardless of whether compensation is involved. Employees must receive approval from their Line Manager and Head – Risk prior to accepting an OBA. Directors of the company must advise the Chair of their Board of Directors prior to taking on any OBAs. Subject to any local regulatory requirements, prior approval is not required to serve on boards of charities or small, private family-holding companies that have no relation to the company. For

greater clarity, approval is not needed to serve on the board of a family holding company which is an extension of one's personal business affairs; however, it is needed to serve on the board of a private operating business with significant operations. When in doubt whether you need to obtain permission, consult with Head – Risk.

Avoid situations in which your personal interest's conflict with the interests of the company or others as clients of the company.

A "conflict of interest" for this purpose occurs when a person's private interest inclines the person, consciously or unconsciously, or appears to incline the person to act in a manner which is not in the interests of the company. You may have a conflict of interest if you are involved in any activity that prevents you from performing your duties to the company properly, or that may create a situation that could affect your ability to act objectively, effectively and in the best interests of the company, including due to among other things, personal interest or receipt of benefits from our relationships with companies, business partners, counterparties, investment banks, brokerage firms, service providers, and other constituencies. Accordingly, you must place the company's interest in any business matter ahead of any personal interest. Remember that the company's interest includes the company's obligations to its clients.

The best way to judge whether you may have a conflict of interest is to ask yourself whether a well-informed person would reasonably conclude that your interest activity or close personal relationship could in any way influence your decision or performance in carrying out a duty on behalf of the company.
To avoid conflicts of interest, identify potential conflicts when they arise and contact Head - Risk if you are unsure whether a conflict exists. In addition, if you become aware of any conflict or potential conflict of another director, officer or employee, you should consult with Head – Risk or the MD, as appropriate.
You may also have a conflict of interest or the appearance of a conflict of interest as a result of a "close personal relationship" with another employee/off roll at the company. To ensure that these relationships are managed appropriately, and to deal with any possible conflicts of interest in an appropriate and responsible manner, you are expected to disclose the existence of such relationships to your Human Resources department.

For the purposes of the Code, a close personal relationship includes, but is not limited to, relationships with a parent or parent equivalent (e.g., adoptive parent), close relative or friend, spouse, fiancée, common law, or anyone else with whom you are in, or have been in, a romantic or intimate relationship.

Do not take corporate opportunities as your own personal opportunities.

You are prohibited from taking personal advantage of a business or investment opportunity that you become aware of through your work at PIL. You owe a duty to the company to advance its interests when the opportunity arises, and you must not compete with the company in any way.

POSITIVE WORK ENVIRONMENT

Be committed to our respectful work environment free from discrimination[3], violence[4] and harassment[5].

The company is committed to promoting equal opportunities and diversity in the workplace. We value diversity, equity and inclusion, and we should all do our part to maintain our respectful work environment where everyone feels safe, included and productive. The company does not tolerate workplace discrimination and harassment. Personnel must work to ensure that the company is a safe and respectful environment where high value is placed on integrity, fairness and respect. For more information on our commitment to a positive work environment, refer to the company's Positive Work Environment Policy.

You have a duty to report discrimination, violence and harassment.

If you experience or become aware of what you believe to be discrimination, violence or harassment, you have a duty to report it in accordance with the "Reporting Potential Code Violations" section of the Code [and/or in accordance with the Positive Work Environment Policy]. Reports of discrimination, violence or harassment will be taken seriously and investigated.

If you are found to be harassing, acting or threatening to act violently towards, or harassing any individual, or if you knowingly condone the discrimination of, violence towards, or harassment of another individual, you will face corrective action up to and including termination without notice and for cause.

We want to create a culture of reporting when it comes to discrimination, violence and harassment, as reporting is essential for us as a company to stamp out these behaviors. While we reserve the right to take corrective action if you knowingly make a false accusation about an innocent party, you will not face retaliation for making a good faith report or assisting in the investigation of a report.

Be committed to ensuring the health and safety of Personnel.

We all have the right to work in an environment that is safe and healthy. In this regard, you must:

a. comply strictly with all occupational, health and safety laws and internal procedures;
b. not engage in illegal or dangerous behavior, including any acts or threats of violence;
c. not possess, distribute or be under the influence of liquor or drugs while on company premises or when conducting company business; and
d. not possess or use weapons or firearms or any type of combustible material in the company's facilities, or at company-sponsored functions

If you or someone you know is in immediate danger of serious bodily harm, first call local law enforcement authorities and then report the incident in accordance with the "Reporting Potential Code Violations" section of the Code

SUSTAINABILITY MANAGEMENT

We believe that value creation and sustainable business practices are complementary goals. We manage our company by combining economic goals with responsible citizenship. This is consistent with our longstanding philosophy and experience that conducting business with a long-term perspective in a sustainable and ethical manner maximizes value. It also requires maintaining a disciplined focus on integrating and operating with robust sustainability principles and practices. Our S***ustainability principles*** codifies our strategy of integrating to sustainability considerations into decision-making. It is based on the following guiding principles:

1. Mitigate the impact of our operations on the environment:
    a. Strive to minimize the environmental impact of operations and improve efficient use of resources over time.
    b. Support the ambition of reaching net zero greenhouse gas (GHG) emissions by 2050 or sooner.
2. Strive to ensure the well-being and safety of our workforce:
    a. Foster a positive work environment based on respect for human rights, valuing diversity, and having zero tolerance for workplace discrimination, violence or harassment.
    b. Operate with robust health and safety practices to support the goal of achieving zero serious safety incidents.
3. Uphold strong governance practices:

a. Operate to the highest ethical standards by conducting business activities in accordance with our Code of Business Conduct and Ethics.
b. Maintain strong stakeholder relationships through transparency and active engagement.

4. Be good corporate citizens:
    a. Strive to ensure the interests, safety and well-being of the communities in which we operate are integrated into our business decisions.
    b. Support philanthropy and volunteerism by our Personnel.

HUMAN RIGHTS AND ANTI-MODERN SLAVERY

We are committed to conducting business in an ethical and responsible manner, including by carrying out our activities in a manner that respects fundamental human rights and supports the prevention of human rights violations within our business including but not limited to:

a. operating with leading health and safety practices to support the goal of zero serious safety incidents.
b. Striving to ensure that the interests, safety and well-being of the communities in which we operate are integrated into our business decisions.
c. fostering a positive work environment based on respect for human rights, valuing diversity and having zero tolerance for workplace discrimination, violence or harassment; and; .
d. operating to the highest ethical standards by conducting business activities in accordance with our Code of Business Conduct and Ethics

We strive to embed these standards into our core business activities, including training, communications, contracts and due diligence processes as appropriate. These practices extend to our interactions with our key suppliers and other business partners. For more information, please refer to the company's Anti-Modern Slavery and Human Trafficking Policy.

---

2 Discrimination" means the differential treatment of an individual or group based on prescribed characteristics protected by l aw. Prescribed characteristics generally include age, color, race, religion, gender, marital status, ancestry, sexual orientation , national origin, and/or disability. It does not matter whether discrimination is intentional; it is the effect of the behavior that matters.

3 Violence" means an action (oral, written or physical) which causes, is intended to cause, could reasonably be interpreted as a threat to cause, or is capable of causing death or bodily injury to oneself or others, or property damage.

4 "Harassment" means conduct which is known or ought reasonably to be known to be unwelcome

and includes contact (e.g., comment s and actions) which would be perceived by a reasonable person as being hostile, humiliating or abusive or cause him/her torment. Harassment covers a wide range of conduct and includes sexual harassment, bullying and psychological harassment.

COMPLIANCE WITH LAWS, RULES, REGULATIONS AND POLICIES

Know and comply with all laws, rules, regulations and policies applicable to your position.

The company is committed to compliance with applicable laws, rules, regulations and policies. Many of our company's activities are governed by laws, rules, regulations and policies that are subject to change. If you have questions about the applicability or interpretation of certain laws, rules, regulations or policies relevant to your duties at the company you should consult with the company's internal legal counsel. In the event a local law, custom or practice conflicts with the Code you must adhere to whichever is most stringent. If you know of any of our practices that may be illegal, you have a duty to report it. Ignorance of the law is not, in general, a defense to breaking the law. We expect you to make every reasonable effort to become familiar with the laws, rules, regulations and policies affecting your activities and to comply with them. If you have any doubts as to the applicability or interpretation of any of the above, you should obtain advice from the company's Head- Risk or internal legal counsel.

Do not trade in securities of the parent company or in any other publicly- traded securities if you possess material non-public information.

While at the Company, you may have access to or become aware of material[9] non-public information either about the parent company or a related or unrelated publicly - traded entity. You must not use this information to gain a financial advantage for yourself or others, either by way of making a trade for yourself, "tipping" others on the information (i.e., disclosing the information to others such as relatives or friends), or otherwise. Doing so is not only a violation of the Code that will result in immediate termination for cause but is also a serious violation of securities laws and will expose any individuals involved to potential civil and criminal prosecution.

Prohibitions on trading in PIL securities shall apply during the quarterly trading restriction period relating to the release of its earnings or when it is in a special trading window closure period as per Code of Conduct for Prohibition of Insider Trading. The trading window for dealing on securities of the Company is closed from the end of each quarter till 48 hours after declaration of financial results. Information on the trading restriction period is intimated from time to time by the Company Secretary.

Do not give or receive bribes, including "facilitation payments".

We value our reputation for conducting business with honesty and integrity. It is vital for us to maintain this reputation as it generates confidence in our business by our stakeholders, which ultimately means it is good for business. We do not pay bribes in furtherance of our business, either directly or indirectly, and you are not permitted to pay bribes on our behalf or authorize others to pay bribes on our behalf. This commitment comes from the highest levels of management, and you must meet this standard.

---

[6] Information about an entity is "material" if there is a substantial likelihood that a reasonable investor would consider the information important when deciding to buy, sell or hold that entity's securities or if the information would reasonably be expected to result in a change in the market price or value of the securities. Information is "non -pubic" until it has been generally disclosed to the public and adequate time has passed for the securities markets to analyze the information. If you are not sure whether the information is material or non-public, consult with your internal legal counsel for guidance.

[7] Facilitation payments are small payments made to secure or speed up routine actions or otherwise induce public officials or other third parties to perform routine functions they are otherwise obligated to perform, such as issuing permits, approving immigration documents or releasing goods held in customs. This does not include legally required administrative fees or fees to fast-track services.

A bribe is anything of value that is offered, promised, given or received to improperly influence a decision or to gain an improper or unfair advantage in promoting, enhancing, obtaining or retaining business. Bribery may not always be in the form of cash payments and may take many other forms, including gifts, travel, hospitality, political contributions, charitable donations, lobbying payments, sponsorships, employment opportunities, internships, and secondments. Facilitation payments[7] are also a form of bribe and are therefore not permitted. For further details, refer to the company's Anti-Bribery and Corruption Policy.

Giving or receiving gifts/entertainment should be reasonable, and in certain cases prohibited.

Gifts and entertainment given to or received from persons who have a business relationship with the company are generally acceptable, if the gift or entertainment is modest in value, appropriate to the business relationship, and does not create an appearance of impropriety. No cash or cash equivalent payments should be given or received. In addition, gifts must not be given to or received from public officials, except for Diwali gifts as prescribed in the Gift Entertainment and Hospitality Policy. Personnel who do not comply with these requirements may be required to reimburse the company for the value of any gifts or benefits they make or receive on behalf of the company and may be subject to disciplinary action up to and including termination for cause. Refer to company's Gifts **,** Entertainment and Hospitality and Anti-Bribery and Corruption Policy for further details.

Political donations to political candidates, political parties and public officials is prohibited.

The donation of funds, whether direct or indirect, to political parties, public officials, political campaigns and / or candidates for political office, with resources of the Companies, is strictly prohibited. Political donations made by individuals on their own behalf should comply with local laws and regulations

We must prevent the use of our operations for money laundering or any activity that facilitates money laundering, the financing of terrorism, or other criminal activities.

The company is strongly committed to preventing the use of its operations for money laundering, the financing of terrorism, or other criminal activities, and will take appropriate actions to comply with applicable anti-money laundering laws.

Jurisdictions may publish lists of individuals and organizations that the company is prohibited from accepting funds from or distributing funds to under applicable anti-money laundering laws. Employees are expected to use reasonable care to verify that counterparties are not owned or controlled by, or acting on behalf of, sanctioned governments, groups, individuals or others. This includes requiring counterparties to make anti-money laundering representations in documents with the company, which Head – Risk or internal legal counsel (or legal counsel of our parent company) can provide upon request.

We must comply with all sanctions laws applicable in the jurisdictions in which we operate.

The U.S. and other jurisdictions and international organizations utilize economic sanctions to promote national security or advance foreign policy objectives. These sanctions prohibit companies from conducting business with certain countries, individuals or entities. Restricted activities may include transfers of assets, monetary payments, provision of services, financial dealings, exports and imports and travel to certain countries.

Our parent company and we are required by law to comply with sanctions restrictions applicable in the jurisdictions in which we operate and in other jurisdictions, such as the U.S., where such laws have extra jurisdictional reach.

You should consider your rights and obligations when providing information to governmental authorities.

Either during or following your employment or directorship at PIL you may be contacted by governmental authorities (e.g., law enforcement, securities regulators, etc.) who are seeking confidential information you obtained through your association with PIL. Whether you are able to respond to these questions or not, we strongly recommend that, for your own protection, you do not speak with authorities without consulting your supervisor and the MD on your rights and obligations, as well as those of the company. In case the situation requires, the MD may seek legal advice as deemed necessary.

Notwithstanding the foregoing, nothing in the Code prohibits or restricts you in any way voluntarily (or upon request) communicating with, or providing information to any government authority, agency or regulator regarding any potential violations of law, rule or regulation, or from making other disclosures that are protected pursuant to applicable whistleblowing rules and regulations. For further information, refer to the *Whistleblowing Policy*.

You have internal reporting obligations in the event you are convicted of a felony or misdemeanor.

We are only as good as our people, and therefore our reputation depends on the reputation of the individuals who serve the company as Personnel. Our screening process at PIL is rigorous and includes background checks so that we have the best information possible about our prospective Personnel. Once at PIL, we expect you to continue to adhere to these principles of openness, honesty and transparency. If at any time while you are associated with the company you are convicted of a felony or misdemeanor or are involved in any conduct that you think may be relevant to your reputation, you have an obligation to report this information to internal legal counsel or your supervisor so that it may be appropriately documented internally.

REPORTING POTENTIAL CODE VIOLATIONS

You are strongly encouraged to make good faith reports.

Internal reporting is critical to the company's success, and it is both expected and valued. You are required to be proactive and promptly report any suspected violations of the Code, or any illegal or unethical behavior or misconduct that you become aware of or are involved with. When making a report, please include specific details and back-up documentation where feasible in order to permit adequate investigation of the concern or conduct reported. Vague, non-specific or unsupported allegations are inherently more difficult to pursue.

Personnel are expected to report actual or potential misconduct or violations of the Code to their supervisor in the first instance, since their supervisor is generally in the best position to resolve the issue. Alternatively, you may contact the company's Head – Risk to report any actual or potential Code violations, or if you have any specific or general questions. Directors should promptly report violations to the Chair of their Board of Directors.

If you have questions about securities laws contact Company Secretary and for the company's whistle blower policy, contact Head – Risk

In the event you do not want to report violations to your supervisor, human resources, or Head – Risk, you can always report through the company's reporting hotline.

Our reporting hotline (the "Reporting Hotline") is managed by an independent third party. The Reporting Hotline allows anyone to call anonymously (if they so choose) to report suspected unethical, illegal or unsafe behavior in English, Marathi, Kannada, Gujarati and Hindi. The Reporting Hotline is available, 24 hours a day, 7 days a week. If you choose to make an anonymous report, your anonymity will be protected to the fullest extent possible as permitted by law.

Hotline Details:	
Number	000-800-0502-070
Website	pipelineinfra.ethicspoint.com

Complaints will be kept confidential and will be dealt with appropriately.

The confidentiality of reported violations will be maintained to the fullest extent possible, consistent with the need to conduct an adequate review and subject to applicable law. You may wish to identify yourself to facilitate our investigation of any report; however, you can make an anonymous report through the Reporting Hotline. The party receiving the initial report must record its receipt, document how the situation was dealt with and file a report with an internal audit, which will be retained for the record. The MD will report all illegal and unethical conduct in violation of the Code to the Company's Board and the Chief Internal Auditor of our parent company and externally in accordance with applicable laws.

We prohibit retaliation against anyone who reports suspected violations of the Code or any law or regulation.

No retribution or retaliation will be taken against any person who has filed a report based on the reasonable good faith belief that a violation of the Code or any law or regulation has occurred or may in the future occur; however, making a report does not necessarily absolve you (if you are involved) or anyone else of the breach or suspected breach of the Code. The company reserves the right to discipline you, if you provide false information or make an accusation you know to be untrue. This does not mean that the information that you provide has to be correct, but it does mean that you must reasonably believe that the information is truthful and demonstrates at least a possible violation of the Code. If you believe that you have been unfairly or unlawfully retaliated against, you may file a report with Head – Risk or Head – HR, or your supervisor, or through the Reporting Hotline.

You are required to cooperate in any internal investigation

Personnel are required to cooperate in any internal investigation into allegations of illegal or unethical behaviour or misconduct. In connection with an internal investigation, you must provide honest, accurate and complete information.

DISCIPLINARY ACTION FOR CODE VIOLATIONS

Please note that we reserve the right to take disciplinary action for Code violations that fits the nature and particular facts of the violation. This could include immediate termination for cause and, if warranted, legal proceedings may be brought against you.

STATEMENT OF COMPLIANCE

Upon joining PIL personnel will be provided with a copy of the Code and required to sign an acknowledgement. The acknowledgement is maintained by the HR- Hiring team. On an annual basis, Personnel will be required to re - certify compliance with the Code. Annual execution of a Statement of Compliance with the Code [and policies referred therein] shall be a condition of your continued directorship or employment with the company.

WAIVERS

A waiver of the Code will be granted only in very exceptional circumstances. A Code waiver for PIL's personnel must be approved by the MD. A Code waiver for a director, officer or employee may be granted in accordance with PIL's policies as consistent with the Code

AMENDMENTS

PIL's Board of Directors reviews and approves the Code on at least an annual basis and is ultimately responsible for monitoring compliance with the Code.

CONTACT INFORMATION

INTERNAL CONTACTS

For any queries or clarification on Code of Business Conduct and Ethics, you may reach out to:

Nilesh Salatry, *Head – Risk*
Nilesh.Salatry@pipelineinfra.com or

Akhil Mehrotra, MD

Akhil.Mehrotra@pipelineinfra.com

LEGAL NOTICE

The company reserves the right to modify, suspend or revoke the Code and any related policies, procedures, and programs at any time. The company also reserves the right to interpret and amend the Code and these policies in its sole discretion. Any amendments to the Code will be disclosed and reported as required by applicable law.

Neither the Code, nor any of the policies referred to herein, confer any rights, privileges or benefits on any employee, create an entitlement to continued employment at the company, establish conditions of employment for the employee, or create an express or implied contract of any kind between employees and the company. In addition, the Code does not modify the employment relationship between employees and the company.

The Code is posted on our website and intranet. The version of the Code on our website and intranet may be more current and supersedes any paper copies, should there be any discrepancy between paper copies and what is posted online.

SCHEDULE A

Pipeline Infrastructure Limited, EnCap Investment Manager Private Limited and Pipeline Management Services Pvt. Ltd. (PMSPL)

CODE OF BUSINESS CONDUCT AND ETHICS

STATEMENT OF COMPLIANCE

All directors, officers and employees must complete this Statement of Compliance

I have received, reviewed and understood the Code of Business Conduct and Ethics (the "Code") of [Pipeline Infrastructure Limited / EnCap Investment Manager Private Limited / Pipeline Management Services Pvt. Ltd.] (the "company")

I hereby agree to comply with the Code, including its provisions for nondisclosure of information both during and after appointment or employment.

To the best of my knowledge;

☐ I am not involved in any situation that conflicts or might appear to conflict with the Code.

☐ I have promptly disclosed to Head Risk, all conflicts or potential conflicts with the Code that I have been involved in since the date of the last Statement of Compliance signed by me and such conflicts have been resolved to the company's satisfaction.

I also agree to notify my supervisor immediately of any change that might adversely affect my compliance with the Code.

Name: _____
(Please print)

Company: _____

Position Title: _____

Branch/Department: _____

Location: _____

Date and Signature: _____ _____
(mm/dd/yy) (Signature)