

CODE OF CONDUCT

Version 2.0

August 2026

1. Introduction

This Code of Conduct Policy (the “**Code**”) is applicable to DEA TopCo LP, DEA TopCo II LP, and its wholly owned and/or controlled, direct and indirect subsidiaries, associates, and joint ventures (hereafter, “**we**,” “**our**,” “**us**,” the “**Company**,” or “**Digital Edge**”), including all full-time, part-time, fixed-term, or temporary employees and other third parties performing work for or on our behalf, including contingent workers, agents, contractors, consultants, directors, officers, and Board members (collectively, “**Company Personnel**,” “**Employee**,” or “**Personnel**”). The Company will encourage its joint venture companies to adopt this Policy as a model or use a similar policy which meets similar standards set forth herein. Digital Edge also expects its suppliers and business partners to follow our Business Partner Code of Conduct.

Company Personnel are expected to act lawfully, honestly, ethically, and in the best interests of the Company while performing work for or on behalf of the Company. If a law conflicts with a policy in this Code, you must comply with the law; however, if a local custom or practice conflicts with this Code, you must comply with the Code. Each of us is responsible for knowing and understanding the policies and guidelines contained in this Code.

Because some of the principles described in this Code may be general in nature, the Code will not provide an answer to all questions or situations that may arise in your day-to-day business activities. If you have a question that the Code does not address directly, you should use your own common sense of what is right based on the standards set forth in the Code, and seek appropriate guidance from others, including the Company’s Compliance Officer, Head of Legal and Compliance.

If you manage people, you have an even greater responsibility. Lead by example, making sure your team members know the Code and that there is no difference between what you do and what you expect from others. Create the kind of workplace where Company Personnel feel comfortable coming forward with questions and concerns and support them when they raise issues. And never retaliate against Company Personnel for sharing concerns in good faith and prevent retaliation by others.

If you have questions, ask them; if you have ethical concerns, raise them. The Head of Legal and Compliance, who is responsible for overseeing and monitoring compliance with this Code, Compliance Officer and the other resources set forth in this Code, are available to answer your questions and provide guidance and for you to report suspected misconduct. In most cases, your manager should be your first point of contact. He or she is likely in the best position to understand your concern and take the appropriate action. If you are uncomfortable speaking with your manager, or if you have already shared a concern and feel it is not being addressed appropriately, please raise your concern through the Digital Edge Ethics Hotline: Email: whistleblower@digitaledge.com. In the event of any doubt, question, or conflict regarding the interpretation or application of this Code, Company Personnel may reach out to the Compliance Officer (vishal.jain@digitaledge.com) or the Head of Legal and Compliance (joe.b@digitaledge.com) for guidance and resolution.

2. Conflicts of Interest

Company Personnel are expected to use their judgment to act always in the best interests of the Company while performing their job duties. As such, Company Personnel should attempt to avoid actual or apparent conflicts of interest.

A conflict of interest exists when your personal interests interfere with the best interests of Digital Edge. For example, a conflict of interest may occur when you or a family member receive a personal benefit because of your position with Digital Edge. Similarly, a conflict of interest may also arise from your personal relationship with a customer, supplier, vendor, competitor, business partner, or other Company Personnel, if that relationship impairs or may be perceived to impair your objective business judgment. Other specific areas of

potential conflict of interest such as external business relationships, serving on boards, personal investments, gifts, entertainment, corporate opportunities, and certain personal relationships with other Company Personnel are discussed in more detail below.

The best rule for any situation that appears to present a conflict of interest is to “abstain and disclose”.

If it is not possible to avoid participating in the event or activity creating the conflict, (1) promptly disclose the potential conflict to your supervisor and contact the Legal Department and (2) avoid participating in decisions that might raise the appearance of a conflict until you receive appropriate guidance from the Company. The Company will consider the facts and circumstances of the situation to decide whether corrective or mitigating action is appropriate.

Some specific potential conflicts of interest to be mindful of are as follows:

a. Outside Business and Consulting Engagements

Company Personnel must obtain approval from the Company prior to (1) beginning any employment, business, or consulting relationship with another company that is a current or potential competitor of Digital Edge or that otherwise has a business relationship with Digital Edge, or (2) accepting any teaching engagements with an educational institution, establishment, or other organization. In addition, you should avoid conducting Digital Edge business with members of your family or others with whom you have a significant personal or financial relationship without the prior approval of the Company.

For further information, please refer to the Company’s Conflict of Interest Policy.

b. Serving on Boards

We encourage Company Personnel to be active in industry and civic associations. However, Company Personnel who serve on boards of directors or advisory boards of any entity or organization are required, prior to acceptance, to obtain approval from the Company.

For further information, please refer to the Company’s Outside Directorship Policy.

c. Investing in Other Companies

Any passive investment of not more than five percent (5%) of the total outstanding shares of a publicly traded company is permitted without Digital Edge approval, provided that the investment is not so large financially (either in absolute dollars or percentage of your total investment portfolio) that it creates the appearance of a conflict of interest. However, any investment in more than two percent (2%) of a public company or any investment in a private company that is a current or potential competitor of Digital Edge or that has a business relationship with Digital Edge requires prior approval from the Company. Digital Edge reserves the right to review and revisit any prior investment approvals to avoid an actual or apparent conflict of interest. Digital Edge may periodically conduct an inquiry of Company Personnel to determine the status and circumstances of board memberships or investments, and Digital Edge Personnel are responsible for continually monitoring and reporting any change in circumstances that might give rise to an actual or apparent conflict of interest.

For further information, please refer to the Company’s Conflict of Interest Policy.

d. Gifts & Entertainment

Giving or receiving gifts or entertainment to or from a current or future client or business partner can potentially create a conflict of interest, especially if the value of the item is significant. Accepting or providing gifts (such as company-branded swag or simple gift baskets) is generally fine if the market value of the item is de minimis and the gift is reasonable and customary and does not inappropriately bias future decision-

making about working with the client or partner or create an appearance of impropriety. Additionally, accepting or providing certain business entertainment (such as an invitation to attend a local cultural or sporting event, or a celebratory meal with a business partner) can be appropriate, provided that the entertainment or meal is reasonable and customary and in the furtherance of a business relationship, the cost is not excessive, and it will not inappropriately bias future decision-making about working with the partner or create an appearance of impropriety.

You should never give or receive cash, cash equivalents (such as gift cards), loans, or any item that obligates you to provide something in return, and you should never actively solicit gifts or entertainment from a current or potential client or business partners.

While you cannot give anything of value to a government official to get or keep business or gain an improper advantage, you may provide modest gifts, meals, and entertainment to government officials where there is a legitimate purpose, and the thing of value is not being provided in exchange for any action or inaction by the official.

For guidance on giving and receiving of anything of value, please see the Company's Anti-Bribery and Anti-Corruption Policy, Gift & Entertainment Policy and Corporate Hospitality and Travel Hosting Policy.

If you plan to expense any gift or entertainment to be provided to a client or business partner, please also see the Company's Business Travel & Expense Reimbursement Policy.

e. Corporate Opportunities

Company Personnel may not exploit or take advantage of business opportunities that are discovered while working at the Company or by using its property or information for personal gain unless the opportunity is disclosed fully in writing to the Company's Legal Department and the Company declines to pursue such opportunity and specifically authorizes (in writing) the pursuit of such opportunity by the disclosing Company Personnel.

f. Potentially Conflicting Relationships

Digital Edge does not prohibit dating among Company Personnel, nor does it prohibit relatives from working together within, for, or on behalf of the Company. However, if a potentially conflicting relationship, romantic or otherwise, involves two employees in a direct reporting relationship, in the same chain of command, or otherwise creates an actual or apparent conflict of interest, the employees must disclose the relationship to Human Resources. While both employees have a responsibility to disclose any such potential conflict, if you are a manager, your failure to properly disclose may result in a more serious disciplinary outcome.

Upon learning of any potential conflict, Digital Edge may reassign at least one of the individuals to a different position or role within the Company. In any event, where your significant other, relative, or any other potentially conflicted person is within your chain of command, you must recuse yourself from any decision-making concerning the person's compensation, promotion, discipline, or termination and must refrain from participating in his/her performance review. Failure to do so may result in disciplinary action taken against you, up to and including termination of your employment with Digital Edge.

If you have a personal or financial relationship with any service providers to Digital Edge, such as vendors, suppliers, or contingent workers, for which you have work-related responsibilities (e.g., where you are participating in vendor selection, determining the terms of a contract or assignment, etc.) you must disclose that relationship to the Legal Department and recuse yourself from any decision-making regarding that service provider.

Digital Edge's Board of Managers (the "**Board**") may from time to time adopt separate policies with respect to board members' conflicts of interest in order to address the particular circumstances arising from their role as members of the board and to comply with the terms of the Limited Partnership Agreement. Any such policy will supersede the conflicts of interest guidelines above to the extent applicable.

For further information, please refer to the Company's Conflict of Interest Policy.

3. Harassment, Discrimination and Workplace Violence

Digital Edge does not tolerate unlawful harassment or any mistreatment (including sexual harassment or discrimination) by or of Company Personnel, guests, clients, or agency partners in the workplace or in a work-related situation, particularly on the basis of sex, race, color, nationality, ethnic or national origin, ancestry, citizenship, religion (or belief, where applicable), age, physical or mental disability, medical condition, sexual orientation, veteran status, marital status, genetic information or characteristics (or those of a family member), or any other category protected under applicable federal, state, or local law.

We are dedicated to maintaining a creative, culturally diverse, and supportive work environment, and do not tolerate discrimination of employees or non-employees with whom we have a business, service, or professional relationship. This applies to all interactions where you represent Digital Edge. Furthermore, we do not tolerate workplace violence of any kind.

If you witness or otherwise suspect harassment, discrimination, or workplace violence has occurred, you are encouraged, and managers are required, to promptly notify (either in writing or verbally) either Human Resources, the Head of Legal and Compliance, or contact our Ethics Hotline.

For further information, please refer to our Dignity in the Workplace Policy.

4. Drugs and Alcohol

Our position on substance abuse is simple: It is incompatible with the health and safety of our employees, and we do not permit it. Consumption of alcohol is not banned at our offices, however, Company Personnel are expected to use good judgment and never drink in a way that leads to impaired performance or inappropriate behavior, endangers the safety of others, or violates the law. Illegal drugs in our offices or at sponsored events are strictly prohibited. If a manager has reasonable suspicion to believe that an employee's use of alcohol (or drugs) adversely affects an employee's job performance or the safety of the employee or others in the workplace, the manager may request an alcohol and/or drug screening, where permitted by law. A reasonable suspicion may be based on objective symptoms such as the employee's appearance, behavior, or speech.

5. Communications

You should take care to ensure that all business records and communications, including electronic communications, are clear and accurate. Electronic communications include, but are not limited to, email, messaging, video conferencing, chat rooms, phone, and fax. The Company may have obligations to preserve electronic communications and other information in connection with existing or reasonably foreseeable legal matters, such as litigation, investigations, subpoenas, or enforcement proceedings. Upon direction from the Legal Department (known as a Legal Hold Notice), you must not alter, delete, or destroy electronic communications or information subject to a Legal Hold Notice.

Please remember that your business communications may be shared or become public through these legal events or publication in the media. Potential risks from inaccurate or misleading statements include, but are not limited to, misrepresentation, breach of contract, and antitrust violations, not to mention embarrassment for the author of the communications.

You must consult with the Communications Department and your CXO before making formal statements or providing information about Digital Edge, our products, or our business and fellow Company Personnel to journalists, bloggers, and industry analysts through any public forum (such as a tradeshow or conference).

You may not give an endorsement or other statement on behalf of Digital Edge or personal endorsement that identifies your affiliation with Digital Edge, except when approved by the Communications Department or the Legal Department. In addition, you may not discuss Digital Edge's business, including financial condition, business or financial performance, products, or business prospects, with financial analysts or actual or potential investors without the prior approval of the Finance Department.

All requests for a representative of Digital Edge to participate in a financial conference (including speaking on a panel or attending a dinner or any event that targets the financial community) must be referred to the CFO for review and managing. If any such analysts or investors contact you, please refer such inquiries to jon@digitaledge.com.

For further information, please refer to our Communications Policy and IT Security Policy.

6. Disclosures

Digital Edge is committed to the transparency and integrity of its financial reports and other communications. Our Chief Executive Officer, Chief Financial Officer, Head of Finance, and people who perform similar functions are deemed our "**senior financial officers**" and are responsible for ensuring that the disclosure in Digital Edge's financial reports is full, fair, accurate, timely, and understandable.

7. Financial Integrity and Responsibility

Company Personnel are expected to act responsibly and exercise sound judgment with respect to financial matters involving the Company. If, in the course of your duties, you spend money or distribute anything else of value, enter contracts, or maintain financial records on behalf of Digital Edge, you must keep accurate and complete records, submit accurate and complete reports as required, and comply with our systems of internal controls, including controls relating to the proper review and internal approvals in respect of such matters.

When you submit an expense for reimbursement or spend money on the Company's behalf, make sure that the cost is reasonable, directly related to the Company's business, and supported by appropriate documentation. Always record the business purpose and comply with other expense reimbursement requirements (e.g., if you take someone out for a business dinner, always record full names, titles and companies of the people who attended, as well as the reason for the dinner).

If you are uncertain about whether you should spend money or submit an expense for reimbursement, check with your manager. Managers are responsible for all money spent and expenses incurred by their direct reports and should carefully review such spend and expenses before approving. Also, each time you enter a business transaction on behalf of the Company, there should be documentation recording that agreement, which is required to be approved by the Legal Department.

Do not sign a contract on behalf of the Company unless all the following are met:

- You are authorized to do so under the Company's Delegation of Powers Policy. If you are unsure whether you are authorized, ask your manager.
- The agreement has been approved by the Legal Department. If you are using an approved Company form contract, you do not need further Legal approval unless you have made changes to the form or are using it for other than its intended purpose.

- You have studied the contract, understand its terms, and have decided that the contract is in Company's interest.

All contracts should be in writing and should contain all relevant terms to which the parties are agreeing – the Company does not permit undisclosed side agreements, oral or written. All completed contracts should be sent to the Legal Department for proper filing and administration.

For further information on the topics raised in this section, please refer to our Delegation of Powers Policy, Contracting Guidelines, Business Travel & Expense Reimbursement Policy, and Purchasing Policy.

8. Confidential Information

Digital Edge's confidential business information is an asset that all Company Personnel must protect. Company Personnel may only use Digital Edge's confidential information for business purposes and must always keep such information in strict confidence. This responsibility extends to confidential information of third parties that we have received under non-disclosure agreements. Confidential information includes data and information, including, without limitation, proprietary data, trade secrets and know-how such as software and product designs, product plans, inventions, processes, designs, drawings, engineering, customer lists, employee data (other than your own), financial information, budgets, pricing, business plans, or other business information.

Your obligation to maintain the confidentiality of this information means that you may not share any such information outside of Digital Edge unless Digital Edge has appropriate non-disclosure agreements in place with the intended recipient.

For help in establishing such an agreement, or if you have questions about provisions of a non-disclosure agreement already in place, or if you have questions about whether certain information can be disclosed, please contact the Legal Department.

Company Personnel should also refrain from sharing confidential information internally beyond those persons who legitimately need to know it for purposes of their job. We have an open and transparent culture, and this is not intended to stifle the ongoing conversation and sharing that has facilitated so much of our success. Rather, you should use your judgment to share what is appropriate inside the Company in furtherance of your and others' jobs. Please always keep in mind that improper use or disclosure of confidential business information could seriously damage Digital Edge's reputation with users, business partners and the community, expose us to liability, and cause harm to our business.

In addition, you are not to bring with you, use or disclose to any person associated with Digital Edge, any confidential or proprietary information belonging to any former employer or other person or entity to which you owe an obligation of confidentiality under any agreement or otherwise. Digital Edge does not need and will not use such information, and we will assist you in any way possible to preserve and protect the confidentiality of proprietary information belonging to third parties.

Please note that this Code is not intended to restrict an employee's legal right to discuss the terms and conditions of his/her employment with any third party.

9. Protection of Customer and Personnel Data

Depending on your role at the Company, you may have access to information systems or tools that enable you to view certain information relating to our customers and/or third parties, which would otherwise not be visible to you but for your role at Digital Edge. You may also have access to information systems or tools that enable you to view personal information relating to Company Personnel (including your co-workers). These tools are important and necessary to enable you to perform your work effectively. With that said, it is of the

utmost importance that you treat this data and access to this data with extreme sensitivity and caution. You are only authorized to access this data to the extent it is required for you to do your job. This data is confidential and subject to privacy protections in many jurisdictions. All Company Personnel must review and comply with all privacy-related policies, including our Data Privacy and Access Policy.

To learn about the sensitivity of different types of personnel data, and how to appropriately protect it, please refer to the Company's Data Privacy and Access Policy and Data Handling Guidelines.

10. Protection and Use of Digital Edge Assets

Digital Edge provides Company Personnel with a wide range of assets to help you perform your work on behalf of the Company. These assets include, but are not limited to, computer equipment, mobile devices, communications platforms and software, office and electronic equipment, and facilities. Company Personnel are expected to treat these assets with care and use them only in accordance with the Company's IT Security Policy. This means that assets should be well maintained and not subject to unreasonable use. If something you are using is damaged, please see that it gets fixed. In addition, you should use your judgment in using Company assets for personal matters as these assets are property of the Company and provided for business use. While we recognize that personal use occurs, it should not be excessive and should not interfere with performance of your business duties. If Digital Edge determines that personal use inhibits business use, Digital Edge may request that you adjust your personal use patterns.

For more information, please see the Company's IT Security Policy.

11. Compliance with Laws

Company Personnel are expected to act within the bounds of applicable laws, rules, and regulations of the countries where we do business. The application of these and other laws can be complex and fact dependent. If you have any questions about the applicability or interpretation of any law, rule, or regulation, you should contact the Legal Department.

Here are some of the legal areas to keep in mind:

a. Data Privacy

Company Personnel must comply with all applicable data privacy laws and legal requirements. These include laws governing the collection, access, and use of data, such as the European Union's General Data Protection Regulation (GDPR), People's Republic of China's Cybersecurity Law 2016 and Civil Code, as well as the Personal Information Protection Act of South Korea.

For more information, please contact the Legal Department or refer to the Company's Data Privacy and Access Policy and Data Handling Guidelines.

b. Anti-Corruption

Company Personnel must comply with all anti-corruption laws of the countries in which we do business, including the U.S. Foreign Corrupt Practices Act (FCPA) and United Kingdom Bribery Act, both of which apply globally.

For more information, please refer to our Anti-Bribery and Anti-Corruption Policy.

c. International Trade

Company Personnel must also comply with all applicable international trade laws and regulations. These laws and regulations apply to the import and export of goods and technical data to and from the U.S. and other

countries, transactions or dealings with sanctioned countries and restricted parties, and anti-boycott requests.

For more information, please refer to our Trade Sanctions Policy.

d. Lobbying and Campaign Finance

Company Personnel are prohibited from using Company resources (which includes volunteering during Company-paid work hours) to engage in political lobbying and funding political campaigns.

Campaign finance laws vary across jurisdictions and apply generally when Digital Edge makes political contributions or engages on policy issues with government entities, elected officials, and candidates for public office. Given the complexity of these laws and the consequences of non-compliance, the Company has elected not to participate in political activities or in the financing of political campaigns.

e. Competition

Digital Edge is committed to competing in a fair and vigorous manner, in compliance with all applicable antitrust and competition laws. Antitrust laws protect consumers by prohibiting anticompetitive conduct that can restrict free competition. In accordance with these laws and regulations, Company Personnel must never agree, either directly or indirectly, with competitors: (1) to set any aspect of prices or other terms related to the products or services we provide to third parties; (2) to allocate customers, territories, or product markets; (3) not to deal with a particular company; or (4) on bid levels or whether to submit a bid on any prospective business.

Further, some additional conduct may be considered unfair or illegal in certain circumstances, including:

- The sharing of competitively sensitive information with competitors;
- Leveraging market power to gain an unfair competitive advantage;
- Requiring a purchaser to resell a product at or above a particular price;
- Entering into agreements with suppliers or customers that impose exclusivity obligations; and
- Requiring customers to purchase one product to get access to another product.

For more information, please refer to the Company's Competition Policy.

f. Money Laundering

Money laundering occurs when individuals or organizations try to conceal illicit funds or make those funds look legitimate. Money laundering is illegal and strictly prohibited by Digital Edge. In certain countries, we are required to report suspicious activity. If you deal directly with customers or vendors, the following examples may signal potential money laundering:

- Attempts to make large payments in cash,
- Payments by someone who is not a party to the contract,
- Requests to pay more than provided for in the contract,
- Payments made in currencies other than those specified in the contract, or
- Payments from an unusual, non-business account.

For further information, please refer to our Anti-Money Laundering Policy and our KYC Policy and Procedures.

g. Insider Trading

Under the various securities laws around the world, it is generally illegal to trade in securities while in the possession of material non-public information about a company in which you are trading securities. It is also generally illegal to provide material non-public information to others who then trade on the basis of that information.

For further information, please refer to our Insider Trading Policy.

h. Environmental, Health and Safety

Digital Edge is committed to complying with environmental, health, and safety (EHS) laws and regulations in the workplace and in the communities where we operate. Our EHS Program is designed to protect the environment, maintain a secure workplace, and provide Company Personnel with the necessary resources to comply with or exceed all applicable EHS laws, rules and regulations and ensure a safe and healthy work environment.

For further information, please refer to our Environmental, Social and Governance Policy and Health & Safety Policy.

12. Reporting Violations, Scope, and Investigation

12.1 Reporting Violations

If you see or suspect anything illegal or unethical, it may seem easier to look the other way or let someone else take the lead - but misconduct affects everyone. You are encouraged, and managers are required, to share your concerns to the individuals mentioned in Section 1 of this Code.

Regardless of who you contact, you can be confident that you are doing the right thing and that your concern will be handled promptly and appropriately. Digital Edge will investigate reports of misconduct thoroughly, disclosing information only to those who need it to resolve the issue. You may be required to cooperate fully with any investigation, but should not investigate independently, as alleged violations may involve complex legal and factual issues, and you may risk compromising the integrity of a formal investigation.

Conduct that violates the law or Company policies, as well as your failure to report a known violation of law or Company policy by someone else, is grounds for prompt disciplinary or remedial action. Discipline for a violation of Digital Edge policies or applicable law may range from a warning up to and including summary termination of employment or relationship with Digital Edge. In addition, Digital Edge may be required or opt to report possible violations of law to and cooperate with appropriate governmental authorities.

12.2 Investigation

Upon receipt of a complaint / information, the Head of Legal and Compliance and Compliance Officer jointly assess it and, where warranted, commence an investigation as per Annexure A. The Compliance Officer and the Head of Legal and Compliance may, in their discretion, adopt a separate investigation procedure appropriate to the nature and circumstances of a specific complaint / matter, in place of the procedure set out in Annexure A. Where they do not exercise that discretion, the procedure set out in Annexure A to this Code shall apply to any complaint concerning a violation of this Code, and to any report or complaint under any other Company policy that does not itself prescribe an investigation procedure.

Investigations are neutral, fact-finding procedures conducted promptly, fairly, and in accordance with the principles of natural justice, and all Company Personnel have a duty to cooperate.

13. Policy Prohibiting Retaliation

We know it takes courage to come forward and share your concerns. We will not nor will we permit others to retaliate against anyone who makes a good faith report about possible misconduct or legal violations or otherwise assists in an investigation of misconduct or legal violation.

14. Training

All Company Personnel, as well as certain third parties as determined by Legal Department, must complete our mandatory training on the Code. Likewise, all Company Personnel will be required to certify their agreement to and compliance with the provisions of the Code, at least annually or more frequently as required by the Company.

15. Amendment and Waivers

This Code is subject to amendment. Any amendment must be approved by the Company's Compensation Committee or, if appropriate, the Board of Managers. Digital Edge's Head of Legal and Compliance may grant waivers under this Code for Digital Edge employees other than executive officers or senior financial officers. Any waiver or modification of this Code for a member of the Board, executive officer, or senior financial officer must be approved by the Board, as a whole.

16. Contact Information:

For any enquiries, questions, concerns, or clarification regarding this Policy, please reach out to:

Compliance Officer
vishal.jain@digitaledgeDC.com

Head of Legal and Compliance
joe.b@digitaledgeDC.com

17. Modifications:

The Company reserves the right to amend or modify this Policy at any time, in order to ensure compliance with applicable laws or to reflect organizational changes.

Any updates to this Policy will be communicated to Company Personnel, and the latest version will be made available on the Company's internal systems or website.

Annexure A

Investigation Procedure

1. Scope
 - a. Applies to complaints and violations reported under this Code and/or other Digital Edge policies in which an investigation procedure is not set out.
2. Reporting Channels
 - a. Report to your manager (if comfortable)
 - b. Or report to Compliance Officer at vishal.jain@digitaledge.com.
 - c. Or via Ethics Hotline.
 - d. If the complaint is against the Head of Legal and Compliance or the Compliance Officer, report it via the Ethics Hotline.
3. Preliminary Review
 - a. Receipt of the complaint shall be acknowledged by the recipient within reasonable time.
 - b. Assess if it falls under this Policy or any other policy, including, but not limited to, POSH (applicable for India).
 - c. Check for conflicts of interest and need for interim safeguards.
4. Investigation Committee
 - a. 3 members: Compliance Officer, HR Head, and one CXO of the concerned subsidiary/joint venture entity of the Company; in case of a complaint against the Compliance Officer and/or Head of Legal and Compliance, the Investigation Committee would be reconstituted by the CEO of the Company.
 - b. Members with conflict must recuse and be replaced.
 - c. Compliance Officer may sub-delegate the investigation proceedings, if required, to an appropriate designated person.
5. Investigation Process
 - a. Interviews with complainant, respondent, and witnesses.
 - b. Review documents, emails, messages etc.
 - c. Complete within 30 business days (extendable with reasons).
 - d. Principle of Natural Justice shall be followed in a strict sense.
 - e. Findings report shall be supplied to all parties involved.
6. Findings and Recommendation
 - a. Committee prepares report: allegations, evidence, findings, and recommendations.
 - b. The Compliance Officer shall, within seven (7) days of completion of the investigation proceedings, submit the report to the Ethics Committee, with a copy to the Head of Legal and Compliance.
7. Appeal Mechanism
 - a. The decision of the Investigation Committee may be appealed to the Ethics Committee by any aggrieved party.
 - b. The Ethics Committee shall comprise the Chief Financial Officer, Head of Legal and

Compliance, and Chief HR Officer of the Company. In case any member of the Ethics Committee is a party to the investigation, then such member shall be replaced by such other Company Personnel as shall be nominated by the Chief Executive Officer of the Company.

- c. Any such appeal before the Ethics Committee will have to be preferred within ten (10) days of receipt of the report from the Investigation Committee.
- d. The Ethics Committee may review the recommendation and, in its discretion, either accept it or, if required, modify or send it back to the Investigation Committee with its observations for re-investigation or reconsideration, as the case may be.
- e. Ethics Committee's decision shall be final and binding on all parties.

8. Implementation and Closure

a. The HR Head of the concerned subsidiary/joint venture entity shall:

- i. communicate the outcome of the investigation to the concerned parties and provide a copy of the investigation report, subject to applicable confidentiality requirements.
- ii. Implement the recommendations of the Investigation Committee/Ethics Committee within 5 business days of the report.

This Annexure A should be read together with, and is subject to, the Company's other policies referenced herein, which shall prevail in the event of any inconsistency.