MARCH 26, 2026

Version 1.0

DIGITAL EDGE POLICY HANDBOOK

DEA TopCo LP ("**Digital Edge**")

Prepared for Employee Reference and Guidance

OBJECTIVE, PURPOSE & PREAMBLE

This **Digital Edge** Policy Handbook ("**Handbook**") has been prepared to provide employees a comprehensive, user-friendly reference guide to **Digital Edge**'s key **Policies** and compliance requirements. It is a compilation of individual **Policies** (referred as "**Policy**" or "**Policies**") of **Digital Edge** which govern DEA TopCo LP and its wholly owned and/or controlled, direct and indirect subsidiaries, associates, and joint ventures ("**Digital Edge or "Company**") and their business operations globally.

The purpose of this Handbook is to:

- Enable easy understanding of **Policies** through simplified summaries, practical guidance, and frequently asked questions.
- Provide quick reference materials for employees in their day-to-day work.
- Promote awareness of compliance obligations and ethical standards.
- Support employees in making informed decisions aligned with Company values and **Policies**.
- Facilitate access to key contact information and reporting channels

This Handbook is designed as a practical tool to help employees navigate **Digital Edge**'s **Policies** framework efficiently. By consolidating essential information from multiple **Policy** documents into a single, accessible resource, we aim to strengthen compliance culture and empower employees to act with confidence and integrity. Any intentional violation of the **Policy** (e.g., failure to follow the guiding principle as mentioned in the **Policy**) is not acceptable and may result in disciplinary action up to and including dismissal of employment with **Digital Edge**.

CONTACTS FOR GUIDANCE

For questions or guidance regarding the Handbook or **Policy**/ies, contact:

Compliance Department: **vishal.jain@digitaledgedc.com**

DISCLAIMER:

This Handbook is provided for ease of reference only and does not replace the respective Policy. All Employees, Personnel and Third Parties must read, understand, and comply with the complete Policy. In the event of conflict between a chapter in this Handbook and the underlying Policy, the underlying Policy shall prevail.

TABLE OF CONTENTS

ANTI-BRIBERY AND ANTI-CORRUPTION POLICY

This section provides a high-level overview of Digital Edge's Anti-Bribery and Anti-Corruption Policy for ease of reference. Employees should refer to the detailed Anti-Bribery and Anti-Corruption Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

The Anti-Bribery and Anti-Corruption Policy ("**Policy**") reflects **Digital Edge's** zero-tolerance approach to bribery and corruption. The **Policy** applies to all Personnel (employees, officers, directors) and Third Parties (business associates, partners, consultants, consultants, agents, intermediaries, representatives, suppliers, contractors, and certain third-party service providers) acting on behalf of **Digital Edge**.

Digital Edge is committed to conducting business with the highest ethical standards and in full compliance with all applicable anti-bribery and anti-corruption laws (ABC Laws), including the U.S. Foreign Corrupt Practices Act (FCPA) and the United Kingdom Bribery Act (UKBA).

Key Principles:

- Absolute prohibition on all forms of bribery and corruption
- No facilitation payments permitted
- Enhanced scrutiny for interactions with public officials
- Mandatory due diligence on Third Parties
- Proper record-keeping and internal controls
- Obligation to report suspected violations
- Mandatory training for all Personnel and certain Third Parties

---

POLICY OBJECTIVE

The **Policy** is designed to:

- Clearly set forth Digital Edge's zero-tolerance stance on bribery and corruption
- Ensure all Personnel and Third Parties understand their obligations when acting on behalf of Digital Edge
- Provide guidance on recognizing potential bribery and corruption issues
- Distinguish acceptable from unacceptable business practices
- Ensure compliance with internationally applicable ABC Laws including the FCPA and UKBA
- Prevent severe civil and criminal penalties, including jail time and reputational harm
- Maintain Digital Edge's commitment to ethical conduct and integrity

Compliance with this Policy and all relevant ABC Laws is a condition of continued employment and/or association with Digital Edge.

DOs AND DON'Ts

DOs

DO conduct all business activities with the highest degree of honesty and integrity

DO read and understand this **Policy** thoroughly

DO ensure gifts, meals, and entertainment are bona fide, moderate and reasonable, infrequent, appropriate, transparent, legitimate, consistent with customary practice, and compliant with applicable laws

DO seek authorization from the Compliance Department before entertaining, contracting with, or offering any benefits or payments to public officials

DO perform appropriate due diligence on Third Parties in accordance with the Third-Party Due Diligence **Policy**

DO record all transactions completely and accurately, and maintain sufficient documentation to support the business purpose

DO maintain books and records for seven (7) years after the transaction

DO promptly report any suspected violations to the Compliance Department or through the Whistleblower **Policy** reporting channels

DO complete mandatory anti-corruption training courses within the notified timeframe.

DO seek guidance from the Compliance Department when in doubt about any business practice or obligation under this **Policy**

DO ensure Third Party agreements include appropriate anti-bribery language

DO obtain written authorization for charitable donations and social contribution payments in accordance with applicable **Policies** of **Digital Edge**

DON'Ts

DON'T offer, promise, authorize, or provide bribes, kickbacks, or anything of value to induce or reward improper performance

DON'T accept bribes or improper payments in any form

DON'T make facilitation payments (small payments to secure or speed up routine actions)

DON'T provide gifts, meals, or entertainment in cash, cash equivalents (gift certificates, coupons), items readily convertible into cash (jewelry, stocks), or contributions to political parties or political candidates

DON'T use **Digital Edge** funds to make political contributions under any circumstances, even if such contributions are permitted by a country's written laws or regulations

DON'T make charitable donations or social contribution payments without proper written authorization

DON'T create or maintain off-the-books accounts

DON'T make false, misleading, or artificial entries in the books and records of **Digital Edge**

DON'T engage Third Parties to do indirectly what you cannot do directly

DON'T ignore red flags or turn a blind eye to potential violations

DON'T retaliate against anyone who reports a suspected violation in good faith

---

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What is bribery and corruption?

A: A bribe is anything of value that is offered, promised, given, or received by any party to influence a decision or to gain or reward an improper or unfair advantage for the benefit of **Digital Edge**. Corruption is the willingness to act dishonestly in return for money or other personal gain. Bribery can take many forms including cash payments, gifts, hospitality, kickbacks, political and/or charitable contributions.

Q2: Who is a "public official" under this Policy?

A: For the purposes of this **Policy**, a "public official" is any officer or employee of a government (including foreign governments), any department, agency, or instrumentality thereof (including government-owned or government-controlled enterprises), officials of public international organizations, persons acting in an official capacity for such entities, foreign political party officials, and candidates for political office.

Q3: Are facilitation payments permitted?

A: No. Facilitation payments are small payments made to secure or speed up routine actions or induce public officials or other Third Parties to perform routine functions they are otherwise obligated to perform. The **Policy** prohibits facilitation payments even though they may be Compliance in certain jurisdictions. This does not include legally required administrative fees or legally permitted fees to fast-track services.

Q4: Can I give or receive gifts, meals, and entertainment?

A: Yes, but only if the benefit is bona fide, moderate and reasonable, infrequent in occurrence, appropriate in nature, transparent, given for a legitimate purpose (related to work or business), consistent with customary practice, and compliant with applicable laws and **Policies** of **Digital Edge**. Cash, cash equivalents, items readily convertible into cash, or contributions to political parties or political candidates are prohibited.

Q5: Can Digital Edge funds be used for political contributions?

A: No. **Digital Edge** funds may never be used for political contributions under any circumstances. The **Policy** does not prohibit employees from voluntarily making personal political contributions on their own time and at their own expense.

Q6: What are the key differences between FCPA and UKBA?

A: The FCPA primarily applies to payments to foreign public officials and imposes accounting provisions on publicly traded U.S. companies. The UKBA prohibits bribery in both public and private sectors, both domestically and internationally, and includes a corporate offence for failing to prevent bribery. The UKBA does not provide specific defences for bona fide business expenses or facilitation payments.

Q7: What happens if I violate this Policy?

A: Violations may result in disciplinary actions up to and including termination of employment and/or association with **Digital Edge** for cause and without notice. **Digital Edge** may also refer violations to appropriate authorities, which could lead to severe civil and criminal penalties including fines, disgorgement, and imprisonment.

Q8: What are the penalties under ABC Laws?

A: Under FCPA, individuals face criminal fines up to $100,000 (or twice the pecuniary gain), imprisonment up to 5 years (or up to 20 years for accounting violations), and civil penalties. Corporations face criminal fines up to $2,000,000 (or twice the pecuniary gain) for anti-bribery violations and up to $25,000,000 for accounting violations. Under UKBA, corporations can face unlimited fines and disgorgement, and individuals can face up to 10 years in prison.

Q9: Am I required to report suspected violations?

A: Yes. Employees and Third Parties have an obligation to promptly report any witnessed behavior that may represent a violation of this **Policy**. Reports should be made to the Compliance Department or through the reporting channels in the Whistleblower Policy of **Digital Edge**. No retaliation will be taken against anyone who reports in good faith.

Q10: What if I'm uncertain whether a payment or practice violates the Policy?

A: Contact the Compliance Department of **Digital Edge** immediately for guidance. It is always better to ask before proceeding with any questionable transaction or practice.

CONFLICT OF INTEREST POLICY

This section provides a high-level overview of Digital Edge's Conflict of Interest Policy for ease of reference. Employees should refer to the detailed Conflict of Interest Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

The Conflict-of-Interest Policy ("**Policy**") reflects **Digital Edge**'s commitment to conducting business in a manner that ensures business judgment and decision-making are not influenced by undue personal interests. The **Policy** applies to all Employees of **Digital Edge**.

A conflict of interest exists if any relationship, influence, or activity impairs an Employee's ability to make fair and objective decisions when performing his or her job or act in the best interests of **Digital Edge**. This definition is construed broadly to include all actual, potential, and perceived conflicts of interest.

Key Principles:

- Proactive identification of conflicts of interest
- Prevention of conflicts wherever possible
- Disclosure and management when conflicts cannot be avoided
- Transparency in decision-making processes
- Protection of **Digital Edge** and Employee reputation
- Compliance with remediation activities

POLICY OBJECTIVE

The purpose of this **Policy** is to enable Employees to easily identify, prevent when possible, or manage identified conflicts of interest. The **Policy** sets a minimum standard that must be followed. Where local laws, regulations, or rules impose a higher standard, that higher standard must be followed.

Conflict of Interest Handling Process:

Identify - Recognize actual, potential, or perceived conflicts of interest

Prevent - Proactively seek to avoid conflicts in day-to-day activities

Unable to prevent? Manage - Disclose and abstain from conflicted decisions

Record and Report - Complete COI Report and submit to Compliance Department

---

DOs AND DON'Ts

DOs

DO act with integrity and exercise good judgment and discretion in your assigned duties

DO act with the requisite degree of independence and objectivity when discharging duties on behalf of **Digital Edge**

DO proactively seek to prevent all conflicts of interest in your day-to-day activities

DO promptly report any situation giving rise to a conflict of interest to your manager (verbally or in writing) as soon as possible

DO take immediate steps to remove or mitigate the conflict of interest

DO complete a COI Report and submit it to the Compliance Department

DO carry out any remediation activities recommended by **Digital Edge**. An Employee's failure to follow the recommended remediation activities may result in disciplinary action, up to an including termination of their employment relationship with **Digital Edge**.

DO abstain from participating in decisions that might raise the appearance of a conflict until you receive appropriate guidance from **Digital Edge**

DO discuss with your manager any work you undertake outside **Digital Edge** (paid or unpaid) that may cause a conflict of interest

DO declare any external company directorship to your Manager in accordance with **Digital Edge**'s Outside Directorship **Policy**

DO inform your new manager of any existing conflict of interest determination if you move to a different assignment within **Digital Edge**

DO seek guidance from the Compliance Department if uncertain about potential conflicts

DON'Ts

DON'T allow personal interests to influence, have the potential to influence, or be perceived to influence your decision-making at **Digital Edge**

DON'T rely solely on your actual state of mind when considering whether a conflict exists - consider whether others may reasonably believe you could have been influenced

DON'T participate in decisions when a conflict of interest exists until you receive appropriate guidance from **Digital Edge**

DON'T fail to disclose actual, potential, or perceived conflicts of interest

DON'T fail to implement recommended remediation activities

DON'T work for, or provide services to, a competitor or potential competitor, customer, or supplier of **Digital Edge**

DON'T foster any relationship with any supplier, customer, competitor, or business partner that compromises your ability to conduct business in the best interests of **Digital Edge**

DON'T influence the decision of **Digital Edge** to place external business with a company owned or controlled by you, your partner, or family members

DON'T own or control more than 1% economic interest (or lower level that might influence your judgment) in entities doing business with **Digital Edge** without disclosure

DON'T use **Digital Edge** assets for personal gain, benefit, or any political activity

DON'T serve as a director of any entity that may be considered a competitor of **Digital Edge**

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What is a conflict of interest?

A: A conflict of interest exists if any relationship, influence, or activity impairs your ability to make fair and objective decisions when performing your job or act in the best interests of **Digital Edge**. This definition is construed broadly to include all actual, potential, and perceived conflicts of interest.

Q2: What is the difference between actual, potential, and perceived conflicts of interest?

A: An actual conflict exists when you are being influenced. A potential conflict could influence you in the future. A perceived conflict exists when others may reasonably believe you could have been influenced, even if you were not actually influenced. All three types must be disclosed and managed.

Q3: What are inherent vs situational conflicts of interest?

A: An inherent conflict is unavoidable and persists indefinitely. A situational conflict occurs unexpectedly, usually in relation to a single event (such as a transaction or selection of service provider) and can usually be managed with a one-off measure.

Q4: What should I do if I identify a conflict of interest?

A: You must (1) promptly report the situation to your manager verbally or in writing as soon as possible; (2) take immediate steps to remove or mitigate the conflict; (3) complete a COI Report and submit it to Compliance Department; and (4) carry out any remediation activities recommended by **Digital Edge**.

Q5: Can I work for another company while employed by Digital Edge?

A: Additional employment outside **Digital Edge** may compromise your ability to fulfill your responsibilities and may breach your employment contract. You must discuss any work you undertake

(paid or unpaid) with your manager. You must not work for or provide services to a competitor, potential competitor, customer, or supplier of **Digital Edge**.

Q6: Can I own shares or financial interests in companies that do business with Digital Edge?

A: You must not own or control more than 1% economic interest (or lower level that might influence your judgment) in entities doing business with **Digital Edge** without proper disclosure. You must not influence the decision of **Digital Edge** to place business with such entities. Any such situation requires completion of a COI Report.

Q7: Can I serve as a director on the board of another company?

A: If you are a director of another entity external to **Digital Edge**, you must declare it to your Manager and also comply with **Digital Edge**'s Outside Directorship Policy. In case of CEO Such a directorship is not permissible if it is with a company which may be considered a competitor of **Digital Edge**.

Q8: What happens after I report a conflict of interest?

A: Your manager will assess the potential conflict in consultation with the Compliance Department and determine if a conflict actually exists. If no conflict exists, you will be informed. If a conflict does exist, the Compliance Department will issue a written conflict of interest determination setting forth restrictions, mitigation measures, or prohibitions. This determination will be sent to you, HR Department, and your manager.

Q9: What if I disagree with the conflict-of-interest determination?

A: You may appeal the determination, which shall be reviewed by either the CFO and/or CEO. Any decision by the CFO and/or CEO shall be deemed final and non-appealable.

Q10: What are the consequences of violating this Policy?

A: Breaches of this **Policy** (e.g., failure to disclose a conflict of interest or failure to implement recommended mitigation procedures) may result in disciplinary action up to and including dismissal of your employment with **Digital Edge**.

EXAMPLES OF POTENTIAL CONFLICTS OF INTEREST

The following examples illustrate common conflict of interest situations:

Outside employment - Working for or providing services to a competitor, customer, or supplier of **Digital Edge**

Ownership and financial interests - Owning or controlling more than 1% economic interest in entities doing business with **Digital Edge**, or influencing **Digital Edge** decisions to place business with such entities

Company assets - Using **Digital Edge** assets for personal gain, benefit, or political activity without proper approval

External Company director - Serving as director of a competitor or entity that creates conflicts with **Digital Edge** responsibilities

Digital Edge joint ventures and subsidiaries - Situations where Personnel serving as directors or representatives of a **Digital Edge** joint venture or subsidiary may face a conflict between their fiduciary duties to the joint venture entity and their responsibilities as Employees of **Digital Edge**.

Relationships with suppliers, customers, competitors - Fostering relationships that compromise ability to conduct business objectively in the best interests of **Digital Edge**

EMPLOYEE RESPONSIBILITIES

- Promptly report situations giving rise to conflicts of interest to your manager
- Take immediate steps to remove or mitigate conflicts
- Complete COI Report and submit to Compliance Department
- Carry out any remediation activities recommended by **Digital Edge**
- Abstain from participating in conflicted decisions until receiving guidance

---

MANAGER RESPONSIBILITIES

- Assess potential conflicts of interest reported or discovered
- Consult with the Compliance Department of **Digital Edge**
- Treat disclosed information with appropriate confidentiality
- Fairly evaluate situations without bias, including risks to business interests and reputation
- Work with Compliance Department to determine best course of action to resolve, manage, or terminate conflicts
- Review on an ongoing basis of any reported conflicts to ensure compliance with remediation activities

---

WHISTLEBLOWER POLICY

This section provides a high-level overview of Digital Edge's Whistleblower Policy for ease of reference. Employees should refer to the detailed Whistleblower Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

The Whistleblower Policy ("**Policy**") reflects **Digital Edge**'s expectation that all Personnel comply with applicable laws, rules, regulations, and internal **Policies** of **Digital Edge**, observing the highest ethical standards. The **Policy** applies to all directors, officers, employees, customers, and/or third-party intermediaries (collectively, **"Personnel"**) of **Digital Edge**.

When there is a known or suspected violation of laws, Policies, or other unethical activities or practices, Digital Edge encourages the reporting of good faith suspicions or concerns and credible information. This Policy provides standards and procedures for reporting concerns and for investigating such reports.

Key Principles:

- Obligation to report material violations of law or internal **Policy**, or any questionable financial, accounting, auditing, or other ethical matter ("**Reportable Matters**")
- Multiple confidential and anonymous reporting channels available
- Good faith reporting required
- Strict prohibition on retaliation against whistle-blowers
- Confidentiality maintained to the extent possible
- Neutral fact-finding investigation process
- Effective remedial action for substantiated violations

POLICY OBJECTIVE

The purpose of this **Policy** is to provide a framework to promote responsible and secure whistleblowing. **Digital Edge** will protect Personnel who raise good faith concerns about serious irregularities within **Digital Edge**.

The Policy is designed to:

- Provide standards and procedures for reporting concerns about violations of laws, **Policies**, or unethical activities
- Establish multiple reporting channels for confidential and anonymous reporting
- Ensure protection from retaliation for whistle-blowers who report in good faith

- Define investigation procedures for reported matters
- Clarify responsibilities of Personnel, supervisors, managers, and investigators
- Ensure effective remedial action for substantiated violations
- Maintain confidentiality to the extent possible

Note: This **Policy** does not create a contract with **Digital Edge**. To the extent a conflict exists between this **Policy** and governing law, governing law shall apply.

DOs AND DON'Ts

DOs

DO report what you believe is a material violation of law or internal **Policy** or any questionable financial, accounting, auditing, or other ethical matter (Reportable Matters)

DO act in good faith and have reasonable grounds for believing the matter raised is a Reportable Matter

DO provide as much detail and be as specific as possible when making a report, including names, dates, description of concern, evidence, and history

DO use designated reporting channels: telephone, email, written report, or direct contact

DO cooperate fully with investigators if you are interviewed or asked to provide information

DO report immediately if you believe you are being subjected to discrimination, retaliation, or harassment for having made a report

DO create an environment (supervisors and managers) in which Personnel can safely and freely raise questions and express concerns

DO watch carefully (supervisors and managers) for indications of unethical or potentially illegal behavior and promptly report such conduct

DO maintain confidentiality of reports and investigations to the extent possible

DO refrain from obtaining evidence if you do not have a right of access

DO understand that you are a reporting party, not an investigator (unless expressly requested by **Digital Edge**)

DON'Ts

DON'T fail to report known or suspected Reportable Matters

DON'T make allegations maliciously, recklessly, with gross negligence, or with foreknowledge that allegations are false

DON'T use this **Policy** to question financial or business decisions that are not Reportable Matters

DON'T use this **Policy** for career-related or other personal grievances

DON'T retaliate, discriminate, or harass any whistle-blower who has raised a Reportable Matter in good faith

DON'T fail to cooperate in an investigation

DON'T deliberately provide false information during an investigation

DON'T withhold, destroy, mutilate, redact, or tamper with evidence if you are subject to an investigation

DON'T influence, coach, or intimidate witnesses if you are subject to an investigation

DON'T interfere with the investigation process

DON'T conduct or participate in investigative activities unless expressly requested by **Digital Edge**

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What are Reportable Matters?

A: Reportable Matters are material violations of law or internal **Policy** or any questionable financial, accounting, auditing, or other ethical matters. Examples include payment of bribes or facilitation payments; providing false or misleading information on financial or public documents; providing false information to or withholding material information from auditors, attorneys, directors, or other representatives; embezzlement, private benefit, or misappropriation of funds; violations of **Digital Edge Policies**; violation of applicable statutes or regulations; and facilitating or concealing any of the above or similar actions.

Q2: How can I make a report?

A: You may make a report through any of the following channels:

(1) Email: Whistleblower@digitaledgedc.com
(2) Written report to: Attn: Chief Legal & Compliance Officer: joe.b@digitaledgedc.com

Q3: Can I make an anonymous report?

A: Yes, a whistle-blower may make a report anonymously to the extent permitted by law. However, you must provide sufficient evidence to justify an investigation. Because investigators cannot interview anonymous whistle-blowers, it may be more difficult to evaluate credibility and less likely to be investigated if the complaint lacks sufficient details.

Q4: What information should I include in my report?

A: Provide as much detail as possible: (1) Who was involved? Include names of employees and/or outside parties; (2) When did it happen? Include dates or time period; (3) What happened? Include reasonable description of the concern; (4) What evidence is there? Attach supporting documentation or describe location of documents; (5) Who should be contacted for more information? This can be another person with additional information; (6) What is the history? Describe prior efforts to address the problem, if any.

Q5: What does "acting in good faith" mean?

A: Acting in good faith means having reasonable grounds to believe the matter raised is a Reportable Matter. Allegations made maliciously, recklessly, or with knowledge that they are false may result in disciplinary action, up to and including termination.

Q6: Will my report be kept confidential?

A: Reports of concern and investigations shall be kept confidential to the extent possible. However, consistent with the need to conduct an adequate investigation, **Digital Edge** cannot and does not guarantee complete confidentiality. All information disclosed during investigation will remain confidential, except as required by law or as necessary to conduct the investigation and take remedial action.

Q7: Will I be protected from retaliation?

A: Yes. **Digital Edge** strictly prohibits discrimination, retaliation, or harassment against any whistle-blower who reports a concern in good faith. Personnel who retaliate may face disciplinary action up to and including termination. However, protection from retaliation does not provide immunity for involvement in the reported misconduct.

Q8: What happens after I make a report?

A: **Digital Edge** will acknowledge receipt of your report within two (2) business days. The Chief Legal and Compliance Officer (CLO) will make an assessment and begin investigation. The CLO will place all Reportable Matters before the Board of Managers. Reports shall be investigated as promptly as is reasonable under the circumstances through neutral fact-finding procedures.

Q9: What are my responsibilities if I am interviewed as part of an investigation?

A: Personnel who are interviewed, asked to provide information, or otherwise participate in an investigation have a duty to fully cooperate with investigators. Your identity will be kept confidential to the extent possible and practicable. You are entitled to protection from retaliation for having participated. You shall be subject to strict disciplinary action up to and including immediate dismissal if you fail to cooperate or deliberately provide false information.

Q10: What happens if a violation is substantiated?

A: If **Digital Edge** determines that a violation has occurred or allegations are substantiated, then **Digital Edge** will take effective remedial action commensurate with the severity of the offense. This

may include disciplinary action against the concerned Personnel, up to and including termination of employment for cause and without notice. **Digital Edge** may also take reasonable measures to prevent further violations and may refer matters to appropriate external regulatory authorities if legally obligated.

INVESTIGATION PROCESS

Acknowledgement: Receipt acknowledged within two (2) business days

Assessment: **Chief Legal and Compliance Officer (CLO)** assess the report and initiates the investigation

Board Notification: CLO places all Reportable Matters before Board

Investigation: Neutral fact-finding procedures conducted promptly and reasonably

Cooperation: All Personnel have duty to cooperate

Confidentiality: Information kept confidential to extent possible

Determination: **Digital Edge** determines if violation occurred or allegations substantiated

Remedial Action: Effective remedial action commensurate with severity of offense

---

REMEMBER

Digital Edge does not tolerate any malpractice, impropriety, statutory non-compliance, or wrongdoing. If you have a good faith suspicion or credible information regarding a Reportable Matter, you must report it. You will be protected from retaliation. When in doubt, speak up.

GIFT & ENTERTAINMENT POLICY

This section provides a high-level overview of Digital Edge's Gift & Entertainment Policy for ease of reference. Employees should refer to the detailed Gift & Entertainment Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

This Gifts & Entertainment Policy ("**Policy**") applies to **Digital Edge** and their business operations globally. This Policy applies to all employees (whether permanent, fixed term or temporary), including contingent workers, agents and its staff, contractors, and consultants providing services on behalf of **Digital Edge** (collectively, "**Personnel**").

Digital Edge recognizes that giving and/or receiving benefits is often a common business or cultural practice. However, benefits must never be used to improperly influence business decisions or obtain an unfair advantage in violation of anti-bribery and anti-corruption laws.

Key Principles:

- Benefits must serve a legitimate business purpose
- Benefits must be transparent, infrequent, and reasonable in value
- Cash and cash equivalents are strictly prohibited
- Pre-approval required for Benefits exceeding specified thresholds
- Enhanced restrictions apply when dealing with Government Officials and State-Owned Entities (SOEs)
- No Benefits during Pending Deal periods
- All Benefits must be properly recorded and disclosed in accordance with the procedures of **Digital Edge**

POLICY OBJECTIVE

The purpose of this **Policy** is to establish the principles, limits, and approval procedures governing the giving and receiving of Benefits with third parties.

The Policy is designed to:

- Prevent bribery, corruption, and improper influence in business interactions
- Establish approval thresholds and procedures for Benefits
- Define prohibited Benefits and activities
- Set annual limits for Benefits involving the same entities
- Promote transparency and accountability in exchange of Benefits
- Protect **Digital Edge** and its Personnel from legal, regulatory, and reputational risks

Note: This **Policy** should be read in conjunction with **Digital Edge**'s Business Code of Conduct, Anti-Bribery and Anti-Corruption **Policy**, Corporate Hospitality and Travel Hosting **Policy**, Charitable Donation and Social Contribution **Policy**, and Business Travel Expense Reimbursement **Policy**.

DOs AND DON'Ts

DOs

DO ensure all Benefits are given/received for legitimate business purposes

DO ensure Benefits are infrequent or occasional in nature

DO ensure Benefits are transparent, open, and accurately recorded

DO ensure Benefits are respectful, customary, and in accordance with local custom

DO ensure Benefits comply with all applicable laws and **Policies** of **Digital Edge**

DO apply your personal judgment in good faith to decide whether a particular Benefit is appropriate

DO seek guidance in advance from the Compliance Department or your direct supervisor if unsure

DO complete Pre-Approval Forms prior to giving or receiving Benefits when required

DO pre-screen all intended recipients for state-ownership/state-control status

DO disclose details of Benefits to Compliance and Compliance and Finance Departments

DO maintain copies of all completed and approved Pre-Approval Forms

DO accurately record full names, titles, companies of recipients, and purpose of the Benefit

DO share Gifts that can be shared (gift baskets, wine baskets) with entire office in common area

DO report violations or suspected violations immediately to your manager or through Whistleblower **Policy** channels

DON'Ts

DON'T give or receive Benefits designed to influence a business relationship or opportunity

DON'T give or receive Benefits to obtain an unfair business advantage

DON'T give or receive Benefits in return for a benefit, advantage, or favor (quid pro quo, kickback, bribe, facilitation payment)

DON'T give or receive lavish or extravagant Benefits

DON'T give or receive embarrassing or inappropriate Benefits (e.g., adult entertainment)

DON'T give or receive prohibited Benefits including cash or cash equivalents, gold or precious metals, watches or jewellery, gift cards or vouchers, stock or stock options, or discounts not available to the public.

DON'T make cash contributions to political parties or candidates (strictly prohibited)

DON'T give or receive any Benefits during Pending Deal periods

DON'T give Gifts to suppliers', customers', or business partners' family members

DON'T provide airfare or flight tickets in conjunction with Entertainment events

DON'T give Entertainment to government regulators, employees, or adjudicators (tax authorities, telecommunications regulators, investigators, data protection authorities)

DON'T accept Benefits from potential vendors or suppliers during contract adjudication period

DON'T intentionally circumvent annual caps by colluding with other employees

---

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What are Benefits?

A: Benefits are anything offered, promised, or given to a recipient, including cash, cash equivalents, Gifts, promotional Gifts, Entertainment, travel, accommodation, business promotional activities, offers of employment, contributions to charities or political parties, investment opportunities, subcontracts, positions in joint ventures, favorable contracts, business opportunities, and other similar items of value to the recipient.

Q2: What are Gifts vs Entertainment?

A: **Gifts** are any item for which a recipient has not paid fair market value, including anything presented as a token, social courtesy, or to commemorate an occasion (holidays, birthdays, special events). Examples: fruit baskets, Diwali sweets, flower bouquets, office stationery, wine, **Digital Edge** branded items. **Entertainment** refers to events attended by both Personnel of **Digital Edge** and third parties to develop better business relationships. Examples: tickets to sporting/music events, golf outings, boat cruises, vacations, trips, dinner and drinks, wine tasting, use of recreational facilities.

Q3: What are Working Meals?

A: Working Meals are meals held on or nearby **Digital Edge**'s or third party's premises before, during, or after a business meeting that are of reasonable value (less than US$75 per person). They are not considered Entertainment but must be declared with list of recipients, names of their employers, and purpose of the business meeting. Working Meals over US$75 per person must be pre-approved under this **Policy**.

Q4: What Benefits are strictly prohibited?

A: The following are strictly prohibited: cash and cash equivalents in any currency; gifts of cash, gold, or precious metals/stones/gems; watches, jewelry, or items readily converted to cash; gift cards, gift vouchers, coupons, pre-paid vouchers; stock or stock options; discounts not generally available to the general public; cash contributions to political parties or candidates.

Q5: What are the approval thresholds for giving Gifts to Commercial Entities?

A: For Commercial Entity employees: US$50 or below = No Pre-Approval; US$50-US$100 = VP and above; US$100-US$250 = CxO. Any Gift greater than these amounts must be additionally approved by the CFO. Annual cap for total value of Gifts given to individual recipients from same Commercial Entity = US$500 per fiscal year (per giver basis).

Q6: What are the approval thresholds for giving Gifts to SOEs and Government Officials?

A: For SOE/Government Official recipients: US$50 or below = VP and above; US$50-US$100 = CxO + CLO. Annual cap for total value of Gifts given to individual recipients from same SOE/Government Official = US$100 per fiscal year (per giver basis).

Q7: What are the approval thresholds for giving Entertainment to Commercial Entities?

A: For Commercial Entity employees: US$150 or below = No Pre-Approval; US$150-US$250 = VP and Above; US$250-US$350 = CxO. Annual cap = Reasonable, consistent with this **Policy**, and infrequent in nature.

Q8: What are the approval thresholds for giving Entertainment to SOEs and Government Officials?

A: For SOE/Government Official recipients: Under US$150 = VP and Above; US$150-US$200 = CxO + CLO. Annual cap for total value of Entertainment given to SOE/Government Officials = US$300 per fiscal year (per giver basis). Personnel of **Digital Edge** are prohibited from giving anything of value to Government Officials except for DE advertising/promotional items of little intrinsic value (US$20 or less, US$50 aggregate per year), modest refreshments, Working Meals and local transportation (US$20 or less per occasion, US$50 aggregate per year), or attendance at widely attended gatherings (requires Compliance Department approval).

Q9: What are Pending Deals and why does timing matter?

A: Pending Deals are opportunities with a third party's company that have been recently closed prior to the invitation/Gift-giving occasion, or deals in the pipeline likely to be closed soon after the invitation/Gift-giving occasion. Giving or receiving Benefits during Pending Deal periods could give the appearance of impropriety and should be avoided. The receipt of Benefits from potential vendors or suppliers should be refused during contract adjudication periods.

Q10: What are the consequences of violating this Policy?

A: Violations of this **Policy** may result in disciplinary action including suspension or termination of employment, as well as other legal or contractual consequences. Failure to accurately record Benefits or obtain required approvals may also result in disciplinary action

---

APPROVAL THRESHOLDS SUMMARY

GIVING OF GIFTS

Recipient Category	**Value of Gift**	**Required Approvers**
Commercial Entities	US$50 or below	No Pre-Approval
	US$50 - US$100	VP and above
	US$100 - US$250	CxO
SOEs/Government Officials	US$50 or below	VP and above
	US$50 - US$100	CxO + CLO

Annual Caps: Commercial Entities = US$500; SOEs/Government Officials = US$100

GIVING OF ENTERTAINMENT

Recipient Category	**Value of Benefit**	**Required Approvers**
Commercial Entities	US$150 or below	No Pre-Approval
	US$150 - US$250	VP and Above
	US$250 - US$350	CxO
SOEs/Government Officials	Under US$150	VP and Above
	US$150- US$200	CxO + CLO

Annual Caps: Commercial Entities = Reasonable and infrequent; SOEs/Government Officials = US$300

RECIEPT OF BENEFITS

Receiving Gifts

Value of Gift	**Required Approvers**
US$50 and below	No Approval
US$50 - US$150	VP and Above
US$150 - US$250	CxO

Annual Cap: US$500 from same entity per fiscal year

Receiving Entertainment

Value of Benefit	**Required Approvers**
US$75 or below	No approval
US$75 - US$250	VP and Above
US$250 - US$ 350	CxO

Annual Cap: No cap, but must be infrequent and consistent with **Policy** guidelines

---

REMEMBER

All Benefits must be transparent, accurately recorded, and comply with this Policy. When in doubt, seek guidance before giving or receiving any Benefit. Cash and cash equivalents are strictly prohibited. No Benefits should be given or received during Pending Deals.

GLOBAL TRADE SANCTIONS POLICY

This section provides a high-level overview of Digital Edge's Global Trade Sanctions Policy for ease of reference. Employees should refer to the detailed Global Trade Sanctions Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

Digital Edge is committed to carrying on its business affairs in a highly ethical manner, including ensuring that **Digital Edge** and its directors, officers, and employees (collectively, "**Personnel**") comply with all applicable trade sanctions laws issued by the United States, the European Union, and the United Nations Security Council (collectively, "**Sanctions Laws"**). This Policy applies to all **Digital Edge** Personnel and sets the standards expected when engaging with third parties acting on behalf of **Digital Edge**.

Key Principles:

- Strict prohibition on dealings with Sanctions Targets
- Thorough due diligence and screening of all Counterparties
- Automated screening process using **Digital Edge**'s GAN Integrity Platform
- Identification and resolution of Red Flags before engagement
- Contractual guarantees with Counterparties to enforce compliance
- Compliance with Export Controls on certain goods, technologies, or materials
- Prompt reporting of suspected violations

Violations of Sanctions Laws can carry severe penalties, including imprisonment, and significant financial fines. Failure to comply with this Policy may result in disciplinary action up to and including termination.

POLICY OBJECTIVE

The purpose of this Policy is to guide Digital Edge's Personnel in complying with all applicable Sanctions Laws and to support Digital Edge's commitment to operating in accordance with such laws. The Policy is designed to:

- Ensure compliance with Sanctions Laws issued by the United Nations, United States, European Union, and other applicable authorities
- Establish due diligence and vetting requirements for all Counterparties
- Define Sanctions Targets and prohibited dealings
- Implement automated screening processes using GAN Integrity Platform

- Identify and address Red Flags before engaging Counterparties
- Establish mitigation practices where enhanced due diligence is required
- Clarify Export Controls compliance requirements
- Require prompt reporting of suspected violations

Violations of this Policy may also constitute violations of applicable Sanctions Laws. Digital Edge reserves the right to report such violations to the appropriate authorities, which may result in penalties, fines, and/or imprisonment.

DOs AND DON'Ts

DOs

DO familiarize yourself with and ensure compliance with this **Policy**

DO conduct thorough risk-based due diligence on all Counterparties

DO obtain minimum required information for all new Counterparties (full legal name, country of residence/incorporation, address, places of business)

DO submit all Counterparties to automated screening process using GAN Integrity Platform

DO complete Counterparty Intake Forms accurately and furnish all requested information

DO focus on recognizing Red Flags raised by Counterparties

DO send screening results identifying Red Flags to **Digital Edge**'s Sanctions Compliance Officer or Compliance Department for review before engaging the Counterparty

DO ensure the Counterparty is not a Sanctions Target, located in a sanctioned country, or owned/controlled by a Sanctions Target

DO obtain contractual guarantees and sanctions provisions with Counterparties

DO promptly contact the Sanctions Compliance Officer if activity may implicate Export Controls

DO promptly report any behavior that may represent a violation of this **Policy**

DO make reports based on reasonable, good faith belief

DO direct questions concerning this **Policy** to the Sanctions Compliance Officer

DON'Ts

DON'T engage with Sanctions Targets or entities located in sanctioned countries **DON'T** engage Counterparties owned, controlled, or acting on behalf of sanctioned governments, individuals, or entities

DON'T engage Counterparties before completing due diligence and screening

DON'T submit incomplete or inaccurate information in Intake Forms

DON'T ignore Red Flags or proceed with engagement until they are reviewed and resolved.

DON'T engage Counterparties who are reluctant to offer information or clear answers on routine commercial issues

DON'T engage Counterparties who appear on Sanctions databases

DON'T engage Counterparties with undisclosed ties to governments or government officials

DON'T export goods, technologies, or materials that may implicate Export Controls without consulting Sanctions Compliance Officer

DON'T fail to report suspected violations of this **Policy**

DON'T retaliate against persons making reports based on reasonable, good faith belief

---

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What are Sanctions Laws?

A: Sanctions Laws are regulations issued by authorities such as the United Nations, United States, and European Union that restrict or prohibit dealings with certain countries, individuals, entities, or organizations ("**Sanctions Targets**"). These measures are typically imposed for foreign **Policy**, national security, or human rights reasons.

Q2: Who are Sanctions Targets?

A: Sanctions Targets are the individuals, entities, organizations, or countries that are subject to restrictions under Sanctions Laws issued by authorities such as the United Nations, United States, or European Union.

Q3: What is a Counterparty?

A: A Counterparty is any third party that **Digital Edge** engages with in business, such as vendors, partners, agents, distributors, or customers. All Counterparties must undergo due diligence and screening before engagement.

Q4: What due diligence is required for Counterparties?

A: Risk-based due diligence must confirm that the Counterparty is not a Sanctions Target, is not located in a sanctioned country, and is not owned or controlled by sanctioned persons. Required information typically includes legal name, address, country of incorporation or residence, places of business, and ownership details.

Q5: What is the screening process?

A: After collecting due diligence information, Personnel must submit the Counterparty for screening through **Digital Edge**'s GAN Integrity Platform. The system checks sanctions databases such as the EU Consolidated List and the U.S. OFAC Sanctions List. Any Red Flags must be reviewed by the Legal Department before engagement.

Q6: What are Red Flags?

A: Red Flags are warning signs that may indicate an increased risk of Sanctions Law violations. Red Flags include: (1) Counterparty's reluctance to offer information or clear answers on routine commercial issues (location of services/sales, beneficial ownership, ties to governments or government officials); (2) Inclusion of the Counterparty, a member of its leadership, or a beneficial owner on searchable Sanctions databases (EU Consolidated List, U.S. OFAC Sanctions List, or similar lists); (3) Undisclosed or suspicious ties to sanctioned countries, governments, or government officials.

Q7: What happens if Red Flags are identified?

A: The matter is reviewed by the Sanctions Compliance Officer or designated Reviewer. Engagement cannot proceed until the Red Flags are resolved or appropriate mitigation measures are implemented.

Q8: What are Export Controls?

A: Export Controls are regulations that restrict the international transfer of certain goods, technologies, or materials, particularly those with potential military or strategic use. Personnel should consult the Sanctions Compliance Officer if such activities may be involved.

Q9: How do I report a violation?

A: Reports should be made pursuant to **Digital Edge**'s Whistleblower **Policy**.

Q10: What are the consequences of violating this Policy?

A: Violations may result in disciplinary action up to and including termination. They may also lead to legal penalties under Sanctions Laws, including significant fines or imprisonment.

SANCTIONS DATABASES

EU Consolidated List of Persons, Groups, and Entities subject to EU financial sanctions:
https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions/overview-sanctions-and-related-tools/en/list

U.S. Office of Foreign Assets Control (OFAC) Sanctions List Search:
https://sanctionssearch.ofac.treas.gov

Any similar list covering Sanctions Targets under applicable law

---

REMEMBER

Digital Edge strictly prohibits dealings with Sanctions Targets. All Counterparties must undergo due diligence and automated screening before engagement. Any Red Flags must be resolved before proceeding. Violations may result in severe penalties, including imprisonment and substantial financial fines. When in doubt, contact the Sanctions Compliance Officer.

BUSINESS CODE OF CONDUCT

HIGH-LEVEL SUMMARY

Under this Business Code of Conduct ("**Code**") 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. Each of us is responsible for knowing and understanding the **Policies** and guidelines contained in this Code.

Key Principles:

- Act lawfully, honestly, ethically, and in the best interests of **Digital Edge**
- Avoid actual or apparent conflicts of interest
- Maintain a workplace free of harassment, discrimination, and violence
- Zero tolerance for drugs and illegal substances in the workplace
- Maintain accurate and complete business records and communications
- Protect confidential information of **Digital Edge** and third parties
- Safeguard customer and personnel data with extreme sensitivity
- Protect and properly use **Digital Edge** assets
- Comply with all applicable laws (data privacy, anti-corruption, trade sanctions, competition, anti-money laundering)
- Report violations promptly without fear of retaliation
- Complete mandatory training and annual certification
- Lead by example if you manage people

If you see or suspect anything illegal or unethical, you are encouraged, and managers are required, to share your concerns. Digital Edge will not tolerate retaliation against anyone who makes a good faith report.

POLICY OBJECTIVE

The purpose of this Code is to provide Company Personnel with a set of common ethical standards that guide conduct in all aspects of business at **Digital Edge**.

The Code is designed to:

- Establish ethical standards for all Company Personnel regardless of level or geographic location
- Guide Company Personnel in acting lawfully, honestly, ethically, and in **Digital Edge**'s best interests
- Define and prevent conflicts of interest in business relationships, board service, investments, and gifts/entertainment
- Prohibit harassment, discrimination, and workplace violence

- Establish drug and alcohol standards for a safe workplace
- Ensure accuracy and integrity of business records and communications
- Protect confidential information and trade secrets of **Digital Edge** and third parties
- Safeguard customer and personnel data in compliance with privacy laws
- Establish proper use and protection of **Digital Edge** assets
- Ensure compliance with all applicable laws, rules, and regulations
- Clarify reporting obligations for suspected violations
- Prohibit retaliation against those who report misconduct in good faith
- Require mandatory training and annual certification
- Empower managers to lead by example and create ethical workplace culture

Violations of this Code may result in disciplinary actions ranging from a warning up to and including summary termination of employment or relationship with Digital Edge in accordance with applicable law.

DOs AND DON'Ts

DOs

DO act lawfully, honestly, ethically, and in the best interests of **Digital Edge**

DO know and understand the **Policies** and guidelines contained in this Code

DO use your common sense of what is right based on the standards set forth in the Code

DO seek appropriate guidance from others, including the Chief Legal and Compliance Officer (CLO)

DO lead by example if you manage people, making sure your team knows the Code

DO create a workplace where Company Personnel feel comfortable coming forward with questions and concerns

DO attempt to avoid actual or apparent conflicts of interest

DO abstain and disclose if a situation presents a potential conflict of interest

DO obtain Company approval before beginning employment, business, or consulting relationships with competitors or business partners

DO obtain Company approval before accepting teaching engagements

DO obtain Company approval before serving on boards of directors or advisory boards

DO obtain Company approval for investments in more than 2% of a public company or any investment in a private competitor or business partner

DO ensure gifts and entertainment are de minimis, reasonable, customary, and do not create appearance of impropriety

DO disclose corporate opportunities discovered while working at **Digital Edge** before pursuing them personally

DO disclose potentially conflicting relationships (romantic or otherwise) involving direct reporting relationships

DO recuse yourself from decision-making concerning compensation, promotion, discipline, or termination of potentially conflicted persons

DO promptly notify Human Resources, CLO, or Ethics Hotline if you witness or suspect harassment, discrimination, or workplace violence

DO use good judgment with alcohol consumption and never drink in a way that leads to impaired performance or endangers safety

DO ensure all business records and communications are clear and accurate

DO preserve electronic communications and information subject to Legal Hold Notices

DO consult with Communications Department and your CxO before making formal statements about **Digital Edge** to media

DO keep accurate and complete financial records and submit accurate reports

DO ensure costs are reasonable, directly related to **Digital Edge**'s business, and supported by appropriate documentation

DO obtain Legal Department approval for all contracts before signing

DO send completed contracts to Legal Department for proper filing and administration

DO protect **Digital Edge**'s confidential business information and use it only for business purposes

DO maintain confidentiality of third-party information received under non-disclosure agreements

DO contact Compliance Department if you have questions about whether certain information can be disclosed

DO access customer and personnel data only to the extent required to do your job

DO review and comply with all privacy-related **Policies** including Data Privacy and Access **Policy**

DO treat **Digital Edge** assets with care and use them only in accordance with IT Security **Policy**

DO contact Legal Department if you have questions about applicability or interpretation of any law

DO share your concerns if you see or suspect anything illegal or unethical

DO cooperate fully with any investigation but do not investigate independently

DO report suspected violations to your manager, business leader, Compliance Department, or Ethics Hotline

DO complete mandatory training on the Code

DO certify your agreement to and compliance with the Code at least annually

DON'Ts

DON'T use your personal interests to interfere with the best interests of **Digital Edge**

DON'T receive personal benefits because of your position with **Digital Edge** (or allow family members to)

DON'T conduct **Digital Edge** business with family members or those with significant personal/financial relationships without prior approval

DON'T serve on boards without obtaining prior Company approval

DON'T invest more than 5% of outstanding shares of publicly traded companies if it creates appearance of conflict

DON'T invest in competitors or business partners without prior Company approval

DON'T give or receive cash, cash equivalents (gift cards), loans, or items that obligate you to provide something in return

DON'T actively solicit gifts or entertainment from clients or business partners

DON'T give anything of value to government officials to get or keep business or gain improper advantage

DON'T exploit or take advantage of business opportunities discovered while working at **Digital Edge** without full written disclosure and authorization

DON'T date or have romantic relationships with direct reports without disclosing to Human Resources

DON'T participate in decision-making for compensation, promotion, discipline, termination, or performance reviews of potentially conflicted persons

DON'T tolerate unlawful harassment, sexual harassment, discrimination, or workplace violence

DON'T discriminate based on sex, race, color, nationality, ethnic origin, religion, age, disability, medical condition, sexual orientation, veteran status, marital status, genetic information, or any protected category

DON'T permit illegal drugs in offices or at sponsored events

DON'T request alcohol/drug screening without reasonable suspicion and where permitted by law

DON'T alter, delete, or destroy electronic communications or information subject to Legal Hold Notices

DON'T make formal statements about **Digital Edge** to media without approval from Communications Department and your CxO

DON'T give endorsements identifying your **Digital Edge** affiliation without approval from Communications or Legal / Compliance Department

DON'T discuss **Digital Edge**'s financial condition, performance, or business prospects with financial analysts or investors without Finance Department approval

DON'T submit expenses for reimbursement that are not reasonable, directly related to Company business, or properly documented

DON'T sign contracts unless you are authorized under Delegation of Powers Policy, contract is approved by Legal Department, and you understand its terms

DON'T enter into undisclosed side agreements (oral or written)

DON'T share **Digital Edge**'s confidential information outside the Company unless appropriate non-disclosure agreements are in place

DON'T bring, use, or disclose confidential or proprietary information from former employers

DON'T access customer or personnel data beyond what is required for your job

DON'T use **Digital Edge** assets excessively for personal matters or in ways that interfere with business duties

DON'T directly or indirectly agree with competitors to set prices, allocate customers/territories/markets, not deal with particular companies, or coordinate bid levels

DON'T share competitively sensitive information with competitors

DON'T leverage market power to gain unfair competitive advantage

DON'T engage in money laundering or accept large cash payments, payments from non-parties to contract, payments exceeding contract amounts, or payments from unusual non-business accounts

DON'T trade securities while in possession of material non-public information

DON'T provide material non-public information to others who then trade on that information

DON'T fail to report suspected violations of law or Company **Policies**

DON'T retaliate against anyone who makes good faith reports about possible misconduct

---

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: Who does this Code apply to and what is expected of me?

A: This Code applies to DEA TopCo LP and its wholly owned and/or controlled direct and indirect subsidiaries (collectively, the **Company** or **Digital Edge**), including all full-time or part-time employees and other third parties performing work for or on behalf of the **Company** on a dedicated basis, including contingent workers, agents, contractors, and consultants. You are expected to act lawfully, honestly, ethically, and in the best interests of the Company while performing work for or on behalf of **Digital Edge**. Each of us is responsible for knowing and understanding the **Policies** and guidelines contained in this Code. 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.

Q2: What is a conflict of interest and how should I handle one?

A: A conflict of interest exists when your personal interests interfere with the best interests of **Digital Edge**. For example, a conflict may occur when you or a family member receives a personal benefit because of your position with **Digital Edge**, or when your personal relationship with a customer, supplier, vendor, competitor, business partner, or other Company Personnel impairs or may be perceived to impair your objective business judgment. The best rule is to abstain and disclose. If you cannot avoid the event or activity creating the conflict: (1) promptly disclose the potential conflict to your supervisor and contact the Compliance Department, and (2) avoid participating in decisions that might raise the appearance of a conflict until you receive appropriate guidance. Specific areas requiring approval include outside business and consulting engagements with competitors or business partners, serving on boards, investing more than 2% in public companies or any amount in private competitors/business partners, and conducting business with family members or those with significant personal/financial relationships.

Q3: What are the rules regarding gifts and entertainment?

A: Accepting or providing gifts or entertainment can potentially create a conflict of interest, especially if the value is significant. Generally acceptable: Company-branded items or simple gift baskets of *de minimis* market value that are reasonable and customary and do not inappropriately bias future decision-making or create an appearance of impropriety; business entertainment such as invitations to local cultural/sporting events or celebratory meals that are reasonable, customary, in furtherance of a business relationship, not excessive in cost, and will not inappropriately bias future decision-making. Never acceptable: cash, cash equivalents (gift cards), loans, or any item that obligates you to provide something in return; actively soliciting gifts or entertainment. For government officials, you may provide modest gifts, meals, and entertainment 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. See the Anti-Bribery and Anti-Corruption **Policy**, Gift & Entertainment **Policy**, and Corporate Hospitality and Travel Hosting **Policy** for detailed guidance.

Q4: What should I do if I witness harassment, discrimination, or workplace violence?

A: **Digital Edge** does not tolerate unlawful harassment (including sexual harassment), discrimination, or workplace violence of any kind. This applies particularly on the basis of sex, race, color, nationality, ethnic or national origin, ancestry, citizenship, religion or belief, age, physical or mental disability, medical condition, sexual orientation, veteran status, marital status, genetic information, or any other category protected under applicable law. 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 CLO, or contact the Ethics Hotline. **Digital Edge** is dedicated to maintaining a creative, culturally diverse, and supportive work environment.

Q5: What is Digital Edge's position on drugs and alcohol?

A: **Digital Edge**'s position on substance abuse is simple: it is incompatible with the health and safety of employees, and is not permissible. Consumption of alcohol is not banned at 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 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 job performance or workplace safety, the manager may request an alcohol and/or drug screening where permitted by law, based on objective symptoms such as appearance, behavior, or speech.

Q6: What are my responsibilities regarding confidential information?

A: **Digital Edge**'s confidential business information is an asset that all Company Personnel must protect. You 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 **Digital Edge** has received under non-disclosure agreements. Confidential information includes proprietary data, trade secrets, know-how (software, product designs, inventions, processes), customer lists, employee data (other than your own), financial information, budgets, pricing, and business plans. You may not share such information outside of **Digital Edge** unless **Digital Edge** has appropriate non-disclosure agreements in place. Contact the Legal Department for help establishing such agreements. You should also refrain from sharing confidential information internally beyond those persons who legitimately need to know it for purposes of their job. Improper use or disclosure of confidential information could seriously damage **Digital Edge**'s reputation, expose the Company to liability, and cause harm to the business. You must not bring, use, or disclose to **Digital Edge** any confidential or proprietary information belonging to any former employer or other person/entity to which you owe an obligation of confidentiality.

Q7: What are my obligations regarding customer and personnel data?

A: Depending on your role, you may have access to information systems or tools that enable you to view certain information relating to customers and/or third parties, or personal information relating to Company Personnel including co-workers. 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. You must treat this data and access this data with extreme sensitivity and caution. All Company Personnel must review and comply with all privacy-related **Policies**, including the Data Privacy and Access **Policy** and Data Handling Guidelines. **Digital Edge** is committed to complying with

all applicable data privacy laws and legal requirements, including 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.

Q8: What laws must I be aware of and comply with?

A: Company Personnel are expected to act within the bounds of applicable laws, rules, and regulations of the countries where **Digital Edge** does business. Key legal areas include: (1) **Data Privacy** – comply with all applicable data privacy laws; (2) **Anti-Corruption** – comply with all anti-corruption laws including US Foreign Corrupt Practices Act (FCPA) and UK Bribery Act; (3) **International Trade** – comply with all applicable international trade laws and regulations on import/export of goods and technical data, transactions with sanctioned countries and restricted parties, and anti-boycott requests; (4) **Lobbying and Campaign Finance** – Company Personnel are prohibited from using Company resources to engage in political lobbying and funding political campaigns; (5) **Competition** – never agree with competitors to set prices, allocate customers/territories/markets, not deal with particular companies, or coordinate bids; (6) **Money Laundering** – do not conceal illicit funds or make funds look legitimate; report suspicious activity; (7) **Insider Trading** – do not trade securities while in possession of material non-public information or provide such information to others who trade; (8) **Environmental, Health and Safety** – comply with EHS laws and regulations.

Q9: How do I report violations of this Code?

A: If you see or suspect anything illegal or unethical, you are encouraged, and managers are required, to share your concerns. You may report to: (1) your manager (in most cases, your first point of contact); (2) your business leader; (3) colleagues; (4) the Compliance Department; or (5) the Company's Ethics Hotline. Regardless of who you contact, you can be confident 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. Conduct that violates the law or **Company Policies**, as well as your failure to report a known violation, is grounds for prompt disciplinary or remedial action. Discipline may range from a warning up to and including summary termination of employment or relationship with **Digital Edge**. **Digital Edge** may be required or opt to report possible violations of law to and cooperate with appropriate governmental authorities.

Q10: Will I face retaliation if I report misconduct?

A: No. **Digital Edge** will not – nor will it 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. **Digital Edge** knows it takes courage to come forward and share concerns. The Company takes all reports seriously, and every report received will be assessed and, where necessary, appropriate investigation will be undertaken. The confidentiality of reported violations will be maintained where possible, consistent with the need to conduct an adequate review and subject to applicable law. Nothing in this Code or **Company Policies** prohibits you from communicating with government agencies about possible violations of local laws or otherwise providing information to government agencies, filing a complaint with government agencies, or

participating in government agency investigations or proceedings, and the Code does not require you to notify the Company of any such communications.

KEY COMPLIANCE AREAS

Conflicts of Interest

- Outside business and consulting engagements with competitors/business partners require prior approval
- Serving on boards of directors or advisory boards requires prior approval
- Investments in more than 2% of public companies or any amount in private competitors/business partners require prior approval
- Conducting business with family members or those with significant personal/financial relationships requires prior approval
- Gifts and entertainment must be de minimis, reasonable, customary, and not create appearance of impropriety
- Corporate opportunities discovered while working at **Digital Edge** must be disclosed before personal pursuit
- Potentially conflicting relationships (romantic or otherwise) involving direct reporting relationships must be disclosed to Human Resources

Workplace Standards

- Zero tolerance for unlawful harassment, sexual harassment, discrimination, or workplace violence
- Discrimination prohibited based on protected categories (sex, race, color, nationality, religion, age, disability, sexual orientation, veteran status, marital status, genetic information, etc.)
- Drug-free workplace – illegal drugs strictly prohibited; alcohol consumption requires good judgment
- Creative, culturally diverse, and supportive work environment maintained

Records and Communications

- All business records and communications must be clear and accurate
- Electronic communications subject to Legal Hold Notices must be preserved
- Formal statements about **Digital Edge** to media require approval from Communications Department and CxO
- Financial reports and disclosures must be full, fair, accurate, timely, and understandable
- Expense reimbursements must be reasonable, directly related to business, and properly documented
- Contracts require Legal Department approval before signing
- All completed contracts must be sent to Legal Department for filing

Information Protection

- Confidential information of **Digital Edge** and third parties must be protected
- Customer and personnel data may only be accessed to the extent required to do your job
- Privacy-related **Policies** must be reviewed and followed.
- **Digital Edge** assets must be treated with care and used in accordance with IT Security **Policy**
- Non-disclosure agreements must be in place before sharing confidential information externally

Legal Compliance

- **Data Privacy:** Applicable Laws
- **Anti-Corruption:** US FCPA, UK Bribery Act
- **Trade Sanctions:** Import/export restrictions, sanctioned countries, anti-boycott
- **Competition:** No price fixing, customer allocation, or sharing competitively sensitive information
- **Money Laundering:** No concealing illicit funds
- **Insider Trading:** No trading on material non-public information
- **Environmental, Health & Safety:** Comply with EHS laws
- **Lobbying & Campaign Finance:** No use of Company resources for political activities

---

REPORTING AND INVESTIGATIONS

How to Report

Report suspected violations to:

- Your manager (first point of contact in most cases)
- Your business leader
- Colleagues
- Compliance Department
- Company's Ethics Hotline

What Happens After Reporting

- **Digital Edge** will investigate reports thoroughly
- Information disclosed only to those who need to resolve the issue
- You may be required to cooperate fully with investigation
- Do not investigate independently

- Confidentiality shall be maintained where possible, consistent with need for adequate review and subject to applicable law

Consequences of Violations

- Conduct violating applicable law or **Company Policies** is grounds for prompt disciplinary or remedial action
- Failure to report known violations is also grounds for discipline
- Discipline may range from warning up to and including summary termination of employment or relationship with **Digital Edge**
- **Digital Edge** may report possible violations of law to governmental authorities

No Retaliation

- **Digital Edge** will not tolerate retaliation against anyone who makes good faith reports or assists in investigations
- Anyone caught or suspected of retaliatory action shall be immediately suspended and have employment terminated
- **Digital Edge** takes non-retaliation very seriously

TRAINING AND CERTIFICATION

All Company Personnel must:

- Complete mandatory training on this Code
- Certify agreement to and compliance with the Code at least annually or more frequently as required

Managers have additional responsibility to:

- Lead by example
- Ensure team members know the Code
- Create workplace where Company Personnel feel comfortable raising questions and concerns
- Support team members when they raise issues
- Never retaliate and prevent retaliation by others

REMEMBER

At Digital Edge, the "how" we do business is just as important as the "what" we do. The Code provides a set of common ethical standards that are simply non-negotiable. Everyone has a role to play in living and adhering to the Code – no matter your level in the Company or geographic location. While the Code is a great resource, it does not cover every situation, so use good judgment in everything you do and ask for help if you are ever unsure. If a business practice does not feel right, speak up. You can raise concerns without fear of retaliation. Do not allow anything to compromise your integrity – not financial targets, not competitive pressures, and not even direct orders from superiors. Know the Code. Understand it. Put it into practice every day.

BUSINESS PARTNER CODE OF CONDUCT

This section provides a high-level overview of Digital Edge's Business Partner Code of Conduct for ease of reference. Business Partners should refer to the detailed Business Partner Code of Conduct available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

The Business Partner Code of Conduct **("Code**") is founded on the principles set forth in **Digital Edge**'s Business Code of Conduct and business partners are responsible for establishing **Policies** and monitoring practices so that all their employees, independent contractors, consultants, and all others who do business for or on their behalf understand and comply with the provisions of this Code.

Key Principles:

- Compliance with all applicable laws, rules, and regulations
- Zero tolerance for corruption, bribery, extortion, kickbacks, or facilitating payments
- Compliance with anti-corruption laws (US FCPA, UK Bribery Act, OECD Convention)
- No money laundering or illicit funds activities
- Compliance with trade restrictions, export controls, and customs laws
- Respect for **Digital Edge**'s Gift & Entertainment and Travel Hosting **Policies**
- Upholding human rights, preventing discrimination, and fair labor practices
- Commitment to health, safety, and a harassment-free workplace
- Fair business, advertising, and competition practices
- Accurate records, reports, and honest dealings
- Protection of privacy, confidential information, and intellectual property
- Environmental responsibility and sustainability
- Whistleblower protection and prohibition against retaliation
- Timely reporting of violations within 3 days

If a situation arises that violates this Code, business partners must report it immediately to Digital Edge's Ethics Helpline.

POLICY OBJECTIVE

The purpose of this Code is to ensure that **Digital Edge**'s business partners share an equally strong commitment to ethical business practices and uphold the same high standards of conduct. The Code is designed to:

- Establish ethical conduct expectations for all business partners
- Ensure compliance with all applicable laws, rules, and regulations
- Prohibit corruption, bribery, extortion, kickbacks, and facilitating payments
- Prevent money laundering and illicit funds activities

- Ensure compliance with trade restrictions, export controls, and customs laws
- Define appropriate conduct regarding gifts, entertainment, and travel
- Uphold human rights and treat workers with dignity and respect
- Prevent discrimination, child labor, and harsh treatment or harassment
- Ensure fair wages, benefits, and working conditions
- Promote health, safety, and drug-free workplace standards
- Maintain fair business, advertising, and competition practices
- Ensure accuracy of records, reports, and honest dealings
- Protect privacy, confidential information, and intellectual property
- Promote environmental responsibility and sustainability
- Establish whistleblower protection and prohibition against retaliation
- Require timely reporting of Code violations within 3 days

Business partners are responsible for monitoring their employees, contractors, consultants, and others acting on their behalf to ensure compliance with this Code.

DOs AND DON'Ts

DOs

DO take time to review this Code, become familiar with it, and draw guidance from it

DO comply with this Code insofar as it relates to your business relationship with **Digital Edge**

DO establish **Policies** and monitor practices to ensure your employees, contractors, consultants, and others comply with this Code

DO act within the bounds of all applicable laws, rules, and regulations

DO conduct activities in full compliance with anti-corruption and anti-bribery laws (US FCPA, UK Bribery Act, OECD Convention)

DO comply with United States export and customs laws and additional export/customs laws in countries where business is conducted

DO understand and ensure compliance with all laws or restrictions for cross-border sale or shipment of products, technologies, or services

DO contact your **Digital Edge** representative or Ethics Helpline before engaging in any activity involving gifts, entertainment, or travel

DO respect **Digital Edge**'s Gift & Entertainment **Policy** and Travel Hosting **Policy**

DO uphold human rights of workers and treat them with dignity and respect

DO maintain a creative, culturally diverse, and supportive work environment

DO pay workers at least the minimum wage required by applicable laws and provide all legally mandated benefits

DO compensate workers for overtime hours at the premium rate required by applicable laws

DO pay workers in a timely manner and clearly convey the basis on which they are being paid

DO maintain accurate records of employee hours worked and wages paid

DO comply with all applicable child labor laws and minimum age requirements

DO exercise diversity in daily business regarding employees and subcontractor selection

DO create safe working conditions and a healthy work environment for all workers

DO comply with all safety regulations

DO commit to a workplace free of harassment and violence

DO uphold fair business standards in advertising, sales, and competition

DO understand and ensure compliance with all competition and trade practices laws

DO collect information on customers and markets only through legitimate means

DO ensure all records and reports provided to **Digital Edge** or government/regulatory bodies are accurate, timely, and compliant with legal standards

DO take appropriate precautions (administrative, technical, physical) to safeguard customers' personal information

DO strictly abide by all nondisclosure agreements and confidentiality agreements

DO immediately notify **Digital Edge** and return any confidential and proprietary information mistakenly received

DO respect intellectual property rights of **Digital Edge** and third parties

DO commit to reducing environmental impact of operations

DO implement conservation measures, recycling, reusing, or substituting materials

DO comply with additional environmental specifications required for **Digital Edge** products and services

DO create programs to ensure whistleblower confidentiality protection

DO have a process for timely correction of any Code deficiencies or violations

DO report any Code violations in good faith as soon as practicable, but in any event within 3 days of identifying such violation

DON'Ts

DON'T directly or indirectly pay, offer, promise to pay, or receive bribes, kickbacks, or facilitating payments

DON'T make small payments to public officials to expedite or secure routine government action (facilitating payments)

DON'T engage in or assist others in concealing illicit funds or money laundering activities

DON'T engage in suspicious payment practices that may indicate money laundering (e.g., unusual payment sources, excessive cash payments, or payments inconsistent with contract terms).

DON'T offer gifts, entertainment, or travel to a **Digital Edge** employee beyond nominal value (retail value US$150 or less)

DON'T offer gifts, entertainment, or travel on a regular or multiple basis

DON'T offer any gift, entertainment, or travel to **Digital Edge** employees involved in RFI, RFP, or contract negotiations processes in which you are participating

DON'T offer to provide travel and accommodations to business or entertainment events (should be at **Digital Edge**'s expense)

DON'T accept cash or non-cash gifts, bribes, or kickbacks from **Digital Edge** employees to influence actions or for any improper purpose

DON'T discriminate against any worker based on race, color, age, gender, sexual orientation, ethnicity, disability, religion, political affiliation, union membership, national origin, or marital status

DON'T require pregnancy tests or discriminate against pregnant workers (subject to applicable law requirements)

DON'T require workers to undergo medical tests that could be used in a discriminatory way (except as required by law or for workplace safety)

DON'T use deductions from wages as a disciplinary measure

DON'T employ child labor in violation of applicable child labor laws and minimum age requirements

DON'T threaten workers with or subject them to harsh or inhumane treatment, including sexual harassment, sexual abuse, corporal punishment, mental coercion, physical coercion, or verbal abuse

DON'T tolerate workplace violence of any kind

DON'T permit business partners to perform work activities for or on behalf of **Digital Edge** while under the influence of drugs or alcohol

DON'T engage in price fixing or agree with competitors to allocate customers

DON'T seek business intelligence by illegal or unethical means

DON'T misstate facts, omit critical information, or modify records or reports to mislead others

DON'T make false representations in connection with **Digital Edge** transactions

DON'T promote or utilize false documentation (non-genuine purchase orders, fraudulent contracts, false records)

DON'T disclose or comment on **Digital Edge** business matters or fail to protect confidential or customer information

DON'T knowingly use the intellectual property of any third party unlawfully

DON'T retaliate against workers who participate in whistleblower programs in good faith or refuse orders violating this Code

DON'T fail to report Code violations as soon as practicable, but in any event within 3 days of identifying such violation

---

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What is the Business Partner Code of Conduct and who does it apply to?

A: The Code outlines the standards **Digital Edge** expects all business partners to follow when conducting business with **Digital Edge**. It is based on **Digital Edge**'s Business Code of Conduct, which applies to employees, officers, and directors and is available at www.digitaledgedc.com. Business partners must comply with this Code in connection with their relationship with **Digital Edge** and ensure their employees, contractors, consultants, and representatives understand and follow its provisions.

Q2: What is Digital Edge's position on corruption, bribery, and kickbacks?

A: Business partners must comply with all applicable anti-corruption and anti-bribery laws, including without limitation the **U.S. Foreign Corrupt Practices Act (FCPA)**, the **UK Bribery Act**, and the **OECD Anti-Bribery Convention**. Business partners must not directly or indirectly offer, promise, pay, or receive bribes, kickbacks, or facilitation payments from any person, whether a public official or private party. "Bribes" involve offering anything of value to gain an improper advantage. "Kickbacks" are payments made after a transaction as a reward for securing business. "Facilitation payments" are small payments made to public officials to expedite routine government actions.

Q3: What are the rules regarding gifts, entertainment, and travel?

A: Business partners must follow **Digital Edge**'s Gift & Entertainment **Policy** and Travel Hosting **Policy**. Gifts, entertainment, or travel offered to **Digital Edge** employees must be of nominal value (US$150 or less) and should not be frequent. No gifts, entertainment, or travel may be offered to employees involved in an RFI, RFP, or contract negotiation in which the business partner is participating. Travel and accommodation for business events should be paid by **Digital Edge**, not the business partner. When in doubt, contact your **Digital Edge** representative or the Ethics Helpline before offering any such benefits.

Q4: What is a public official under this Code?

A: A public official is any person who is paid with government funds. This includes individuals who work for a local, state/provincial, or national government, or a public international organization, as well as employees of public government-owned or operated schools and state-owned enterprises. Employees at such organizations are considered public officials regardless of title or position.

Q5: What are money laundering indicators I should watch for?

A: Business partners may not engage in or assist others in concealing illicit funds or money laundering activities. Sample indicators of money laundering that merit further investigation include: (1) Attempts to make large payments in cash; (2) Payments by someone who is not a party to the contract; (3) Requests to pay more than provided for in the contract; (4) Payments made in currencies other than those specified in the contract; (5) Payments from an unusual, non-business account.

Q6: What are Digital Edge's expectations regarding labor and human rights?

A: Business partners must respect workers' human rights and treat them with dignity and respect. Discrimination based on race, gender, religion, nationality, disability, or other protected characteristics is prohibited. Business partners must comply with wage and labor laws, including minimum wage, overtime pay, and legally required benefits. Child labor is strictly prohibited. Partners must also maintain safe working conditions and provide a workplace free from harassment, violence, or inhumane treatment.

Q7: What records and reporting requirements apply to business partners?

A: Business partners must maintain accurate and complete records relating to business conducted with **Digital Edge**. Records and reports provided to **Digital Edge** or regulatory authorities must be truthful, complete, timely, and compliant with legal and financial standards. Business partners must not falsify records, omit important information, or create false documentation related to **Digital Edge** transactions

Q8: What are business partners' obligations regarding privacy and confidential information?

A: Business partners must comply with applicable privacy laws and take appropriate administrative, technical, and physical measures to protect customer personal information from misuse or unauthorized access. They must also comply with all confidentiality and nondisclosure agreements,

avoid commenting on **Digital Edge** business matters, and immediately notify **Digital Edge** of, and return any, confidential information received in error.

Q9: What is Digital Edge's whistleblower protection Policy?

A: Business partners must establish processes to protect whistleblower confidentiality and prevent retaliation against individuals who report concerns in good faith or refuse to participate in activities that violate this Code. Any deficiencies or violations identified through audits or investigations must be addressed promptly.

Q10: How and when must business partners report violations of this Code?

A: Business partners must in good faith report any violations of this Code – whether such violations are their own, another business partner's, or a **Digital Edge** employee's – to **Digital Edge** as soon as practicable, but in any event within three (3) days of identifying such a violation. All such reports should be sent to **Digital Edge**'s Ethics Helpline. If a situation arises that, in the business partner's opinion, violates this Code, the business partner is expected to report it immediately to **Digital Edge**'s Ethics Helpline, identifying themselves as a business partner.

COMPLIANCE AREAS SUMMARY

Anti-Corruption and Anti-Bribery

- Full compliance with anti-corruption and anti-bribery laws (US FCPA, UK Bribery Act, OECD Convention)
- Zero tolerance for bribes, kickbacks, or facilitating payments
- Prohibition applies to public officials and private parties

Trade and Export Compliance

- Compliance with US export and customs laws
- Compliance with additional export/customs laws in countries where business is conducted
- Understanding and compliance with all cross-border trade restrictions

Gifts, Entertainment, and Travel

- Gifts, entertainment, or travel to **Digital Edge** employees limited to nominal value (retail value ≤US$150)
- Never on regular or multiple basis
- No offerings during RFI, RFP, or contract negotiations processes
- Employee travel and accommodations at **Digital Edge**'s expense (not business partner's)

Labor and Human Rights

- Uphold human rights of workers
- No discrimination based on protected categories

- Minimum wage and legally mandated benefits required
- Overtime compensation at premium rates
- Strict prohibition on child labor
- Safe working conditions and healthy work environment
- Workplace free of harassment and violence

Fair Business Practices

- Fair business standards in advertising, sales, and competition
- Compliance with antitrust and competition laws
- No price fixing or customer allocation agreements
- Legitimate means only for collecting business intelligence

Records and Privacy

- Accurate, timely, and compliant records and reports
- No false representations or false documentation
- Protection of customer personal information (administrative, technical, physical safeguards)
- Strict confidentiality of **Digital Edge** information
- Respect for intellectual property rights

Environmental Responsibility

- Commitment to reducing environmental impact
- Conservation measures for water and energy
- Recycling, reusing, or substituting materials
- Compliance with environmental specifications for **Digital Edge** products/services

---

REPORTING VIOLATIONS

All violations of this Code must be reported to **Digital Edge**'s Ethics Helpline and Compliance Department as soon as practicable, but in any event within 3 (three) days of identifying the violation.

REMEMBER

As a valued business partner, you are expected to comply with this Code insofar as it relates to your business relationship with Digital Edge. You are responsible for establishing Policies and monitoring practices so that all your employees, independent contractors, consultants, and all others who do business for or on your behalf understand and comply with the provisions of this Code. If a situation arises that violates this Code, report it to Digital Edge's Ethics Helpline as soon as possible and no later than 3 days after identifying the violation.

TRAVEL, HOSTING AND CORPORATE HOSPITALITY POLICY

This section provides a high-level overview of Digital Edge's Travel, Hosting and Corporate Hospitality Policy for ease of reference. Employees should refer to the detailed Travel, Hosting and Corporate Hospitality Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

This Travel, Hosting and Corporate Hospitality Policy (**"Policy"**) sets forth specific rules and procedures for **Digital Edge**'s provision of Corporate Hospitality and Travel Hosting to third parties. Corporate Hospitality and Travel Hosting in connection with business events require careful management to ensure compliance with local laws and regulations as well as internal **Digital Edge Policies**. This **Policy** is intended to ensure that such activities are legitimate, transparent, and never used to improperly influence third parties or violate anti-corruption laws.

Key Principles:

- **Policy** must be read in conjunction with Gifts and Entertainment **Policy** and Anti-Bribery and Anti-Corruption **Policies**
- Personal judgment in good faith must always be applied to decide whether Corporate Hospitality or Travel Hosting is appropriate
- All third-party attendees must be pre-screened for State-Owned Entity (SOE) or Commercial Entity status
- State-Owned Entities (SOEs) are entities wholly or majority-owned (50% or more) or controlled by government
- Commercial Entities are not owned by SOE or minority owned (less than 50%) by SOE
- Corporate Hospitality events must be organized by Marketing Department
- Corporate Hospitality must have invitees from several different organizations outside **Digital Edge**
- Events must be hosted by **Digital Edge** with multiple **Digital Edge** Personnel in attendance
- Legitimate business purpose required: demonstrating capabilities, business discussions, building relationships
- Events must not be lavish or extravagant, especially Entertainment portion
- Two-stage approval process required: Stage 1 (prior to incurring costs) and Stage 2 (prior to sending invitations)
- Stage 1 and Stage 2 approvals require L1 Approver, CFO, and CLO approval (the L1 Approver is the head of the department for which the event is being organized)
- External speakers, trainers, and event-wide costs not deemed part of per-person costs if reasonable
- No spouses, partners, family members, or plus ones allowed except for customary events under US$350 per person
- Transparency Notice required for all commercial entity invitees

- Transparency Form required for all SOE invitees (must be completed and returned before event, may be obtained through electronic means as well)
- SOE individuals limited to maximum two (2) Corporate Hospitality events per fiscal year
- Travel Hosting poses greater risk and is discouraged – limited to explicitly required and legally permissible situations
- Travel Hosting only allowed for events primarily consisting of demonstrations or business discussions
- Travel Hosting requires reasonable and bona fide business-related expenses directly related to promotion, demonstration, explanation of products/services, or contract execution/performance
- Pre-approval required before committing to Travel Hosting obligations
- Airfare and accommodations must align with **Digital Edge**'s Business Travel and Expense Reimbursement **Policy**
- Travel Hosting approval thresholds: Under US$100 (no pre-approval required if principles satisfied), US$100-500 (VP and above), Above US$500 (CFO and CLO)
- SOE individuals limited to maximum two (2) occasions of Travel Hosting per fiscal year
- First Class airfare never allowed for guests
- **Digital Edge** arranges travel – third parties do not arrange, and **Digital Edge** does not reimburse self-arranged travel
- Cash payments to third parties strictly prohibited except with Compliance Department written approval
- Payment directly to vendors preferred over reimbursement to individuals
- Per diems discouraged – require advance written Compliance Department approval
- Social Contributions/Charitable Donations require Compliance Department background check and CEO/CFO approval
- Social Contributions never used to improperly influence third parties
- Requestors must disclose conflicts of interest with potential charities
- Documentation and receipts must be retained and recorded properly

Digital Edge recognizes situations require Corporate Hospitality and Travel Hosting in furtherance of business objectives. This Policy ensures such events are compliant with local laws and regulations as well as Digital Edge internal Policies and procedures.

POLICY OBJECTIVE

The objective of this **Policy** is to ensure that Corporate Hospitality and Travel Hosting activities are conducted in compliance with local laws and regulations as well as **Digital Edge** internal **Policies** and procedures, while supporting legitimate business objectives.

This Policy is designed to:

- Supplement Gifts and Entertainment **Policy** with specific rules for Corporate Hospitality and Travel Hosting
- Ensure compliance with Anti-Bribery and Anti-Corruption **Policies**
- Require application of personal judgment in good faith for appropriateness of benefits

- Establish pre-screening requirements for all third-party attendees (SOE or Commercial Entity status)
- Define State-Owned Entities (SOEs) as entities wholly or majority-owned (50%+) or controlled by government
- Define Commercial Entities as entities not owned by SOE or minority owned (less than 50%) by SOE
- Require Corporate Hospitality events organized or approved by Marketing Department
- Ensure Corporate Hospitality has invitees from several different organizations outside **Digital Edge**
- Require events hosted by **Digital Edge** with multiple **Digital Edge** Personnel in attendance
- Ensure legitimate business purpose (demonstrating capabilities, business discussions, building relationships)
- Prohibit lavish or extravagant events, especially Entertainment portions
- Establish two-stage approval process (Stage 1 before incurring costs, Stage 2 before sending invitations)
- Require L1 Approver, CFO, and CLO approval for both stages
- Exclude external speakers, trainers, and event-wide costs from per-person calculations if reasonable
- Prohibit spouses, partners, family members, plus ones except for customary events under US$350 per person
- Require Transparency Notice for all Commercial Entity invitees
- Require Transparency Form for all SOE invitees (completed and returned before event)
- Cap SOE individuals at maximum two (2) Corporate Hospitality events per fiscal year
- Discourage Travel Hosting due to increased risk of violation of anti-corruption laws
- Limit Travel Hosting to explicitly required and legally permissible situations only
- Allow Travel Hosting only for events primarily consisting of demonstrations or business discussions
- Require reasonable and bona fide business-related expenses for Travel Hosting
- Require pre-approval before committing to Travel Hosting obligations
- Align airfare and accommodations with Business Travel and Expense Reimbursement **Policy**
- Establish Travel Hosting approval thresholds (Under US$100, US$100-500, Above US$500)
- Cap SOE individuals at maximum two (2) Travel Hosting occasions per fiscal year
- Prohibit First Class airfare for guests
- Require **Digital Edge** arrangement of travel (not self-arranged by third parties)
- Prohibit cash payments to third parties except with Compliance Department written approval
- Prefer direct vendor payment over individual reimbursement
- Discourage per diems – require Compliance Department advance written approval
- Require Compliance Department background check for Social Contributions/Charitable Donations
- Require CEO and CFO approval for Social Contributions/Charitable Donations
- Prohibit use of Social Contributions to improperly influence third parties
- Require disclosure of conflicts of interest with potential charities

- Require documentation retention and proper recording in **Digital Edge** books and records
- Protect **Digital Edge** reputation and ensure compliance with anti-corruption laws

This Policy should be read in conjunction with Digital Edge's Gifts and Entertainment Policy and Anti-Bribery and Anti-Corruption Policies.

DOs AND DON'Ts

DOs

DO read this **Policy** in conjunction with Gifts and Entertainment Policy and Anti-Bribery and Anti-Corruption Policies

DO always apply your personal judgment in good faith to decide whether Corporate Hospitality or Travel Hosting is appropriate

DO pre-screen all third-party attendees for State-Owned Entity (SOE) or Commercial Entity status before event

DO review third party organization's webpage under Investor Relations to determine SOE status

DO understand SOEs are entities wholly or majority-owned (50% or more) or controlled by government

DO understand Commercial Entities are not owned by SOE or minority owned (less than 50%) by SOE

DO ensure Corporate Hospitality has invitees and participants from several different organizations outside **Digital Edge**

DO ensure events are hosted by **Digital Edge** with multiple **Digital Edge** Personnel in attendance (not individual employees)

DO follow two-stage approval process for Corporate Hospitality events

DO submit Stage 1 Pre-Approval Form (proposed agenda, estimated costs, target attendees) to L1 Approver, CFO, and CLO before incurring costs (except event planning agency fees)

DO submit Stage 2 Pre-Approval Form (confirmed agenda, venue, activities, costs, invitee list) to L1 Approver, CFO, and CLO at least five (5) working days before sending invitations

DO ensure all three approvers (L1 Approver, CFO, CLO) approve before proceeding

DO understand external speakers, trainers, and event-wide costs not part of per-person costs if reasonable and per industry rates/standards

DO alert approvers if external speaker/trainer is from entity with Pending Deal (compensation can be viewed as improper Benefit)

DO allow spouses, partners, family members, plus ones only for customary events under US$350 per person (family days, picnics, movie screenings, theatre outings)

DO encourage **Digital Edge** spouses, partners, family members to attend plus one events

DO disclose inclusion of partners and plus ones when seeking pre-approval

DO limit plus ones to approved guest plus one additional person per guest

DO send Transparency Notice to all Commercial Entity invitees with official invitations

DO understand SOE invitees cannot attend if Transparency Form not completed and returned

DO understand Travel Hosting poses increased risk of violation of anti-corruption laws and is discouraged

DO limit Travel Hosting to explicitly required and legally permissible situations only

DO ensure Travel Hosting involves reasonable and bona fide business-related expenses directly related to promotion, demonstration, explanation of products/services, or contract execution/performance

DO obtain all pre-approvals before committing to Travel Hosting obligations

DO allow airfare and accommodations only for events primarily consisting of demonstrations or business discussions (working summits, conferences, round-tables)

DO align airfare and accommodations with Business Travel and Expense Reimbursement Policy (class of travel, room rates, travel expenditures)

DO include Travel Hosting in Stage 1 and Stage 2 approval requests if provided in conjunction with Corporate Hospitality

DO obtain pre-approval for standalone Travel Hosting per Annex A thresholds (Under US$100, US$100-500, Above US$500)

DO limit SOE individuals to maximum two (2) occasions of Travel Hosting per fiscal year

DO mirror **Digital Edge**'s Business Travel and Expense Reimbursement Policy for airfare expenses

DO ensure **Digital Edge** arranges transportation and lodging (not arranged by third parties)

DO limit lodging to accommodation costs and reasonable meal expenditures in business class hotels during meeting/event period only

DO mirror Business Travel and Expense Reimbursement **Policy** parameters and caps for lodging

DO pay only for incidental and local transportation associated with third party participation (standard car only)

DO ensure meals and Entertainment within Travel Hosting are appropriate per **Policy** and ABC Policy

DO ensure initiating **Digital Edge** Personnel ensures meals and Entertainment do not exceed approved amounts

DO pay directly to vendors (airlines, hotels, car rental companies) rather than to third party being hosted

DO require receipts for legitimate permissible expenses prior to reimbursement

DO pay reimbursement to third party organization/Company rather than individual wherever possible

DO obtain advance written Compliance Department approval for payment of per diems (discouraged due to inherent risks)

DO submit completed Pre-Approval Form for Social Contributions/Charitable Donations to Compliance l Department

DO ensure Compliance Department conducts background check confirming entity/charity is bona fide and not controlled by/for benefit of SOE or terrorism conduit

DO submit Pre-Approval Form with Compliance Department approval Memo to CEO and CFO for final approval

DO ensure CEO and CFO approve Social Contributions/Charitable Donations in writing before making donation

DO retain documentation substantiating Social Contributions (receipts) and record properly in **Digital Edge** books and records

DO send copy of approved Social Contribution documentation to Finance Department with payment requisition

DO disclose any existing or potential conflicts of interest with potential charity (e.g., donation to charity owned by customer or customer family member during Pending Deal)

DO store all approvals and Transparency Forms and provide copies to Finance and Compliance Departments upon request

DO adjust non-compliant portions of event if denied by any approver

DON'Ts

DON'T proceed with Corporate Hospitality or Travel Hosting without reading Policy in conjunction with Gifts and Entertainment Policy and ABC Policies

DON'T proceed with Corporate Hospitality or Travel Hosting without applying personal judgment in good faith about appropriateness

DON'T proceed if uncertain about SOE status – contact Compliance Department at least three (3) working days before submission

DON'T organize Corporate Hospitality events without Marketing Department organization or approval

DON'T host events with invitees from only one or two organizations (must be several different organizations)

DON'T allow individual **Digital Edge** Personnel to host events (must be **Digital Edge**-hosted with multiple Personnel in attendance)

DON'T organize Corporate Hospitality without legitimate business purpose

DON'T organize lavish or extravagant events, especially Entertainment portions

DON'T skip two-stage approval process for Corporate Hospitality events

DON'T send invitations before Stage 2 approval obtained (save-the-date notices acceptable)

DON'T proceed without approval from all three approvers (L1 Approver, CFO, CLO)

DON'T submit Stage 2 Pre-Approval Form less than five (5) working days before invitations need to be sent

DON'T include external speakers/trainers from entities with Pending Deal without alerting approvers and including it in the Pre-Approval Request Form.

DON'T allow spouses, partners, family members, plus ones at Corporate Hospitality events except for customary events under US$350 per person

DON'T allow more than one additional plus one per guest at approved plus one events

DON'T send invitations without including Transparency Notice for Commercial Entity invitees

DON'T send invitations without including Transparency Form for SOE invitees

DON'T allow SOE invitees to attend if Transparency Form not completed and returned before event

DON'T allow SOE individuals to attend more than two (2) Corporate Hospitality events per fiscal year

DON'T commit to Travel Hosting without understanding it poses increased corruption risk

DON'T provide Travel Hosting unless explicitly required and legally permissible

DON'T provide Travel Hosting unless it involves reasonable and bona fide business-related expenses

DON'T commit to Travel Hosting without obtaining all pre-approvals first

DON'T provide airfare and accommodations for events not primarily consisting of demonstrations or business discussions

DON'T deviate from Business Travel and Expense Reimbursement Policy for airfare and accommodations

DON'T provide First Class airfare to guests under any circumstances

DON'T allow SOE individuals to receive Travel Hosting more than two (2) occasions per fiscal year

DON'T exceed Business Travel and Expense Reimbursement Policy parameters and caps for lodging

DON'T provide cars at third party disposal for sightseeing or personal use

DON'T use limousines or other extravagant transportation (standard cars only)

DON'T allow meals and Entertainment to exceed approved amounts within Travel Hosting

DON'T make cash payments to third parties to cover travel and travel-related expenses (strictly prohibited except with Compliance Department written approval)

DON'T pay third party being hosted instead of paying vendors directly unless direct payment not possible

DON'T reimburse without receipts for legitimate permissible expenses

DON'T use per diems without advance written Compliance Department approval (discouraged due to inherent risks)

DON'T make Social Contributions/Charitable Donations without submitting Pre-Approval Form to Legal Department

DON'T proceed without Compliance Department background check confirming entity/charity is bona fide

DON'T make Social Contributions/Charitable Donations without CEO and CFO written approval

DON'T use Social Contributions to improperly influence third parties

DON'T fail to disclose conflicts of interest with potential charities

DON'T fail to retain documentation and record Social Contributions properly in **Digital Edge** books and records

DON'T fail to send copy of approved documentation to Finance Department with payment requisition

DON'T fail to store all approvals and Transparency Forms

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What is the scope and purpose of this Policy?

A: This **Policy** is a supplement to the Gifts and Entertainment Policy and applies to **Digital Edge** worldwide operations and all **Digital Edge** Personnel. It sets forth specific rules and procedures for Corporate Hospitality and Travel Hosting to third parties. This **Policy** ensures such activities comply with local laws and regulations as well as **Digital Edge** internal **Policies** and procedures. Personal judgment in good faith must always be applied to decide appropriateness. **Policy** should be read with Gifts and Entertainment Policy and Anti-Bribery and Anti-Corruption Policies.

Q2: What is the difference between State-Owned Entities (SOEs) and Commercial Entities?

A: State-Owned Entities (SOEs) are entities wholly or majority-owned (50% or more) or controlled by government. Review organization's webpage under Investor Relations to determine SOE status. Contact Compliance Department at least three (3) working days before submission if uncertain. Commercial Entities are not owned by SOE or minority owned (less than 50%) by SOE. All third-party attendees must be pre-screened for SOE or Commercial Entity status before event.

Q3: What qualifies as Corporate Hospitality and what is the approval process?

A: Corporate Hospitality events must be: organized/approved by Marketing Department; have invitees from several different organizations outside **Digital Edge**; be hosted by **Digital Edge** with multiple Personnel in attendance; have legitimate business purpose (demonstrating capabilities, business discussions, building relationships); not be lavish or extravagant. Two-stage approval required: Stage 1 (before incurring costs except planning fees) and Stage 2 (at least 5 working days before sending invitations). Both stages require L1 Approver, CFO, and CLO approval.

Q4: What are the rules for spouses, partners, family members, and plus ones?

A: No spouses, partners, family members, or plus ones of external parties are allowed at Corporate Hospitality events except for customary events under US$350 per person (family days, picnics, movie screenings, theatre outings). **Digital Edge** spouses/partners/family members encouraged but not required to attend. Maximum one additional plus one per guest. Inclusion of partners/plus ones must be disclosed when seeking pre-approval.

Q5: What are Transparency Notice and Transparency Form requirements?

A: Transparency Notice must be sent to all Commercial Entity invitees with official invitations. Transparency Form must be sent to all SOE invitees with official invitations. SOE invitees must complete and return Transparency Form before event, otherwise they cannot attend. Forms can be automated through electronic means (e.g., click-through on **Digital Edge** micro-site) provided confirmations retained and available to Compliance Department upon request.

Q6: What are the caps on Corporate Hospitality and Travel Hosting for SOEs?

A: SOE individuals limited to a maximum of two (2) Corporate Hospitality events per fiscal year. SOE individuals limited to a maximum of two (2) occasions of Travel Hosting per fiscal year. These caps ensure compliance with anti-corruption laws and prevent appearance of impropriety.

Q7: When is Travel Hosting allowed and what are the approval thresholds?

A: Travel Hosting poses greater anti-corruption risk and is discouraged. Only allowed when explicitly required and legally permissible for reasonable and bona fide business-related expenses directly related to promotion, demonstration, explanation of products/services, or contract execution/performance. Airfare and accommodations only for events primarily consisting of demonstrations or business discussions. Approval thresholds: Under US$100 (no pre-approval required if principles are satisfied), US$100-500 (VP and above), Above US$500 (CFO and CLO). Must align with Business Travel and Expense Reimbursement **Policy**.

Q8: What are the requirements for airfare, lodging, and transportation?

A: Airfare must mirror Business Travel and Expense Reimbursement **Policy**. First Class airfare is never allowed for guests. **Digital Edge** must arrange travel (not self-arranged by third parties). Lodging limited to accommodation costs and reasonable meals in business class hotels during meeting/event period only. Must follow Business Travel and Expense Reimbursement **Policy** parameters and caps. Local transportation only for incidental needs associated with **Digital Edge** activities. Standard cars only (limousines and extravagant transportation prohibited). No cars at guest disposal for sightseeing.

Q9: What are the payment and reimbursement rules?

A: Cash payments to third parties strictly prohibited (exceptions require Compliance Department written approval). Payment directly to vendors (airlines, hotels, car rental companies) preferred over payment to third party being hosted. If direct payment is not possible, reimbursement requires receipts for legitimate permissible expenses. Wherever possible, pay third party organization/**Digital Edge** rather than individual. Per diems discouraged due to inherent risks – require advance written Compliance Department approval.

Q10: What are the requirements for Social Contributions and Charitable Donations?

A: Submit completed Pre-Approval Form to Compliance Department. Compliance Department conducts background check confirming entity/charity is bona fide and not controlled by/for benefit of SOE or terrorism conduit. If approved by Compliance Department, submit Pre-Approval Form with Compliance Department approval Memo to CEO and CFO. Both CEO and CFO must approve in writing before making donation. Business purpose must be clear with no impropriety or appearance of impropriety. Social Contributions never used to improperly influence third parties. Requestors must disclose conflicts of interest with potential charities (e.g., donation to charity owned by customer/customer family member during Pending Deal). Retain documentation and record properly in **Digital Edge** books and records. Send copy to Finance Department with payment requisition.

CORPORATE HOSPITALITY EVENT REQUIREMENTS

Definition and Qualifying Criteria:

- Organized or approved by Marketing Department
- Invitees and participants from several different and distinct organizations outside **Digital Edge**
- Hosted by **Digital Edge** (not individual **Digital Edge** Personnel) – multiple **Digital Edge** Personnel in attendance
- Legitimate business purpose: demonstrating **Digital Edge** capabilities, holding business discussions, building strong working relationships with multiple third parties
- Not lavish or extravagant, especially Entertainment portion (notwithstanding overall event cost)
- Complies with general principles and parameters of **Policy**

If event for multiple persons with per-person cost within GE Policy limits, can be processed under GE Policy instead.

TWO-STAGE APPROVAL PROCESS FOR CORPORATE HOSPITALITY

Stage 1 Approval (Prior to Incurring Costs)

Timing: Before incurring any costs apart from event planning agency fees

Submission Requirements:

- Event purpose
- Proposed agenda
- Estimated costs (overall and per activity)
- List of target attendees (if known) with name of organization, title, and whether Commercial Entity or SOE

Required Approvers: L1 Approver, CFO, and CLO (all three must approve)

Upon Approval: Marketing Department proceeds with planning and preparation, including booking venue and associated activities

Stage 2 Approval (Prior to Sending Invitations)

Timing: At least five (5) working days before invitations need to be sent

Submission Requirements:

- Confirmed agenda
- Venue
- Activities
- Costs (overall and per activity)

- Invitee list

Required Approvers: L1 Approver, CFO, and CLO (all three must approve)

Upon Approval: Marketing Department may send invitations to approved invitees

If Denied: Marketing Department adjusts non-compliant portions of event

---

TRAVEL HOSTING APPROVAL THRESHOLDS

Value of Benefit	**Required Approvers**
Under US$100	Pre-approval not required (if general principles satisfied)
Between US$100 - US$500	VP and Above
Above US$500	CFO and CLO

All Travel Hosting must be pre-approved even if outlined in contractual commitment with third party.

Digital Edge Personnel must not commit to Travel Hosting obligation without obtaining pre-approvals.

TRAVEL HOSTING GUIDELINES

Airfare

- Must mirror **Digital Edge**'s Business Travel and Expense Reimbursement Policy
- First Class airfare never allowed for guests under any circumstances
- **Digital Edge** arranges transportation (not self-arranged by third parties)
- **Digital Edge** will not reimburse third parties for self-arranged travel

Lodging

- Include only accommodation costs including reasonable meal expenditures
- Business class hotels only
- Only during meeting/facility visit/seminar/event period or en-route
- Must mirror Business Travel and Expense Reimbursement Policy parameters and caps
- **Digital Edge** follows standard expense reimbursement Policies for incidental hotel charges

Local Transportation

- Pay only for incidental and local transportation associated with third party participation in **Digital Edge** activities
- Standard cars only (use of limousines and extravagant transportation prohibited)
- May pay for transport to/from hotel and **Digital Edge** sites including **Digital Edge**-hosted entertainment
- Will not pay for car at third party disposal for sightseeing or personal use

Meals and Entertainment

- Evaluated using criteria in **Policy** and ABC Policy considering overall hosting agenda
- Initiating **Digital Edge** Personnel responsible for ensuring meals and entertainment do not exceed approved amounts

Form of Payment

- Cash payments to third parties strictly prohibited (exceptions require Compliance Department written approval)
- Payment directly to vendors preferred (airlines, hotels, car rental companies) rather than to third party being hosted
- If direct payment not possible, reimbursement requires receipts for legitimate permissible expenses
- Per diems discouraged (require advance written Compliance Department approval)

CAPS ON SOE INDIVIDUALS

- **Corporate Hospitality:** Maximum two (2) events per fiscal year
- **Travel Hosting:** Maximum two (2) occasions per fiscal year

These caps ensure compliance with anti-corruption laws and prevent appearance of impropriety.

SPOUSES, PARTNERS, FAMILY MEMBERS, PLUS ONES

General Rule: Not allowed at Corporate Hospitality events

Exception: Allowed for customary plus one events under US$350 per person

- Family days
- Picnics
- Movie screenings
- Theatre outings

Digital Edge spouses, partners, family members encouraged but not required to attend plus one events.

Disclosure: Inclusion of partners and plus ones must be disclosed when seeking pre-approval.

Limitation: Maximum one additional plus one per guest (approved guest plus one additional person of guest's choice).

EXTERNAL SPEAKERS AND EVENT-WIDE COSTS

Not Deemed Part of Per-Person Costs:

- External speakers
- Trainers
- Event-wide costs (equipment rental, conference room rental)

Conditions:

- Costs must be reasonable
- Demonstratively per industry rates/standards
- Not lavish or extravagant

Special Alert Required:

- If external speaker/trainer from entity with Pending Deal, alert approvers before engagement
- Compensation for speaking/training can be viewed as improper provision of Benefit
- Any donations to speaker's charity of choice must be pre-approved by Compliance Department per Annex B (Social Contributions/Charitable Donations)

SOCIAL CONTRIBUTIONS AND CHARITABLE DONATIONS

Definition: Donations to charities, institutions, governments, or third-party organizations made on behalf of **Digital Edge**.

Approval Process:

1. **Request for Approval:** Submit completed Pre-Approval Form for Giving of Social Contributions/Charitable Donations to Compliance Department

2. **Background Check:** Compliance Department confirms that entity/charity is bona fide and not controlled by/for benefit of SOE or terrorism conduit. Verification may include:

    - Obtaining relevant documents, accountant statements, information on entity/charity purpose and key management
    - Requesting receipts, reports, documents demonstrating how entity will use funds

- Obtaining information from local U.S. Embassy office
- Obtaining written opinion from external counsel
- Checking entity not suspected of supporting terrorism

3. **Compliance Department Approval Memo:** Compliance Department prepares memorandum setting forth findings and either approves or rejects

4. **CEO/CFO Approval:** If approved by Compliance Department, Requestor submits Pre-Approval Form with Compliance Department approval Memo to CEO and CFO for review and approval. Both must approve in writing before making donation.

5. **Record Retention:** Retain documentation substantiating donation (receipts) and record properly in **Digital Edge** books and records. Send copy to Finance Department with payment requisition.

Prohibitions:

- Social Contributions never used to improperly influence third parties
- Requestors must disclose existing or potential conflicts of interest with potential charity
    - Example: donation to charity owned by potential/existing customer or customer family member, particularly during Pending Deal period

---

MARKETING DEPARTMENT RESPONSIBILITIES

For Corporate Hospitality Events:

- Submit Stage 1 completed Pre-Approval Form (purpose, description, estimated costs, venue, proposed itinerary, proposed invitees) to L1 Approver, CFO, and CLO
- Submit Stage 2 completed Pre-Approval Form (overall cost, per event line-item cost, entire itinerary, intended attendees) to L1 Approver, CFO, and CLO at least five (5) working days before invitations need to be sent
- If denied by any approver, adjust non-compliant portion of event
- Send Transparency Notice and Transparency Form with official invitations
- Collect completed and signed Transparency Forms from SOE guests prior to event
- Store all approvals and Transparency Forms
- Send copies to Finance and Compliance Departments upon request

---

TRANSPARENCY REQUIREMENTS

Transparency Notice

- Required for all Commercial Entity invitees
- Sent with official invitations
- Informs invitees of **Digital Edge Policies** and compliance requirements

Transparency Form

- Required for all SOE invitees
- Sent with official invitations
- Must be completed and returned to Marketing Department prior to Corporate Hospitality Event
- SOE invitees cannot attend if form not completed and returned
- Can be automated through electronic means (e.g., click-through on **Digital Edge** micro-site for event) provided confirmations retained by Marketing Department and readily available to Compliance Department upon request

---

CONTACTS FOR GUIDANCE

Compliance Department

Email: vishal.jain@digitaledgedc.com

For questions about:

- SOE status determinations (contact at least 3 working days before submission)
- Corporate Hospitality and Travel Hosting **Policy** interpretation
- Pre-approval requirements and thresholds
- Per diem approvals
- Social Contributions/Charitable Donations background checks and approvals
- Transparency Notice and Transparency Form requirements
- **Policy** compliance and exceptions

Chief Legal Officer (CLO)

For approval of:

- Stage 1 Corporate Hospitality events (with L1 Approver and CFO)
- Stage 2 Corporate Hospitality events (with L1 Approver and CFO)
- Travel Hosting above US$500 (with CFO)

Chief Financial Officer (CFO)

For approval of:

- Stage 1 Corporate Hospitality events (with L1 Approver and CLO)
- Stage 2 Corporate Hospitality events (with L1 Approver and CLO)
- Travel Hosting above US$500 (with CLO)
- Social Contributions/Charitable Donations (with CEO)

Chief Executive Officer (CEO)

For approval of:

- Social Contributions/Charitable Donations (with CFO)

Marketing Department

For:

- Corporate Hospitality event organization and approvals
- Transparency Notice and Transparency Form distribution and collection
- Event planning and coordination

Finance Department

For:

- Payment processing for approved Corporate Hospitality and Travel Hosting
- Social Contributions/Charitable Donations payment processing
- Records retention and accounting

REMEMBER

Corporate Hospitality and Travel Hosting must comply with this Policy, Gifts and Entertainment Policy, and Anti-Bribery and Anti-Corruption Policies. Always apply personal judgment in good faith to decide appropriateness. Pre-screen all third-party attendees for SOE or Commercial Entity status. SOEs are entities wholly or majority-owned (50%+) or controlled by government – contact Compliance Department if uncertain. Corporate Hospitality requires Marketing Department organization/approval, invitees from several organizations, Digital Edge hosting with multiple Personnel, legitimate business purpose, and must not be lavish or extravagant. Follow two-stage approval process: Stage 1 before incurring costs (except planning fees) and Stage 2 at least five (5) working days before sending invitations. Both stages require L1 Approver, CFO, and CLO approval. Send Transparency Notice to Commercial Entity invitees and Transparency Form to SOE invitees (must be completed and returned before event). Limit SOE individuals to maximum two (2) Corporate Hospitality events and two (2) Travel Hosting occasions per fiscal year. Travel Hosting is discouraged due to anti-corruption risks – limit to explicitly required and legally permissible situations. Obtain pre-approvals before committing: Under US$100 (no pre-approval if principles satisfied), US$100-500 (VP and above), Above US$500 (CFO and CLO). Align airfare and accommodations with Business Travel and Expense Reimbursement Policy. Never provide First Class airfare. Digital Edge arranges travel (not self-arranged). Cash payments strictly prohibited except with Compliance Department written approval. Pay vendors directly rather than third parties. Per diems discouraged – require Compliance Department advance written approval. Social Contributions/Charitable Donations require Compliance Department background check and CEO/CFO written approval. Never use Social Contributions to improperly influence third parties. Disclose conflicts of interest with charities. Retain documentation and record properly.

THIRD PARTY DUE DILIGENCE POLICY AND PROCEDURES

This section provides a high-level overview of Digital Edge's Third Party Due Diligence Policy and Procedures for ease of reference. Employees should refer to the detailed Third Party Due Diligence Policy and Procedures available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

This Third Party Due Diligence **Policy** and Procedures **Policy** ("**Policy**") ensures an appropriate level of due diligence is undertaken in respect of all Third Parties with whom **Digital Edge** intends to engage in a business relationship, prior to engaging in that business relationship.

In today's globally connected world, our reputation is as equally important as the quality of our products and services. Third parties are essential to our success, but who we engage with reflects who we are as a **Digital Edge**. We must only deal with third parties who are reputable and prepared to apply the same standards of business conduct as we do ourselves.

Key Principles:

- Third parties essential to **Digital Edge** success and reflect who **Digital Edge** is
- **Digital Edge** must carefully vet third parties before engaging with them
- Third parties include suppliers, distributors, agents, advisors, consultants, and customers
- Companies now held accountable for actions of those acting on their behalf
- **Digital Edge** must ensure third parties are reputable and apply same standards of business conduct
- **Policy** promotes compliance with Business Code of Conduct, Trade Sanctions **Policy**, Anti-Money Laundering, Anti-Bribery Anti-Corruption **Policy**, and applicable laws
- Before entering or renewing relationship with Third Party, Sponsor must comply with **Policy** requirements. A Sponsor should be at the level of E-3 and above to ensure appropriate seniority in respect of the engagement and management of the Third-Party relationship.
- Violations result in disciplinary action up to termination of employment and termination of Third Party engagement
- Due diligence type and robustness vary depending on Level and Risk Rating of Third Party
- Due diligence may include informing Third Parties of **Policy**, meeting to assess character, inquiries into reputation and past conduct, financial checks, background screenings, watch list checks, and obtaining compliance certifications
- All Third Parties subject to **Policy** with different levels of due diligence based on category and Risk Rating
- Third Parties categorized as Level 1 (engaging with others on **Digital Edge** behalf) or Level 2 (dealing only with **Digital Edge**)
- Risk Ratings classified as Very Low, Low, Medium, High, or Very High Risk

- Three levels of due diligence: Basic Due Diligence, Mid-Level Due Diligence, Enhanced Due Diligence
- Process automated through Third-Party GAN Integrity Due Diligence Platform (the "**Platform**")
- Seven-step process: Registration and Pre-Classification, Risk Assessment, Due Diligence, Decision-Making, Post-Approval Contracting, Monitoring, Record Keeping
- All Red Flags must be resolved or mitigated before final approval
- Third Party can only be engaged if approved in Platform and written Agreement entered
- Continuous monitoring through Vantage Screening tool
- Due diligence must be renewed periodically based on Risk Rating
- **Digital Edge** committed to non-retaliation for good faith reporting of violations

Digital Edge recognizes that the third parties we engage in our day-to-day business are essential to our success and reflect who we are. Consequently, we strive to ensure that we only deal with third parties who are reputable and who are prepared to abide by the same standards of business conduct.

POLICY OBJECTIVE

The objective of this **Policy** is to ensure an appropriate level of due diligence is undertaken in respect of all Third Parties with whom **Digital Edge** intends to engage in a business relationship, prior to engaging in that business relationship.

This Policy is designed to:

- Promote compliance by **Digital Edge** with obligations under various laws, rules, and regulations
- Ensure compliance with **Digital Edge Policies** including Business Code of Conduct, Trade Sanctions **Policy**, Anti-Money Laundering, Anti-Bribery Anti-Corruption **Policy**
- Determine type and robustness of due diligence based on Level and Risk Rating of Third Party
- Inform Third Parties and associated companies of **Policy** requirements
- Meet with Third Parties to better assess their character
- Make commercially reasonable inquiries into reputation and past conduct of Third Parties
- Conduct financial checks on Third Parties
- Conduct background screenings and watch list checks on Third Parties
- Obtain compliance certifications from Third Parties
- Classify Third Parties as Level 1 (engaging with others on **Digital Edge** behalf) or Level 2 (dealing only with **Digital Edge**)
- Assign Risk Ratings as Very Low, Low, Medium, High, or Very High Risk
- Perform Basic Due Diligence, Mid-Level Due Diligence, or Enhanced Due Diligence as appropriate

- Utilize Third-Party GAN Integrity Due Diligence Platform for automated process management
- Register Third Parties and conduct pre-classification
- Assess risks systematically through Internal Questionnaires and Third-Party Due Diligence Questionnaires
- Conduct Vantage Screening including negative Internet searches and database checks
- Identify and resolve Red Flags before approval
- Document Final Evaluation and obtain appropriate approvals
- Require written Agreements with mandatory compliance clauses before engagement
- Monitor Third Parties continuously through Platform and event-triggered activities
- Renew due diligence periodically (4 years for Very Low/Low Risk, 3 years for Medium Risk, 1 year for High/Very High Risk)
- Maintain proper record keeping and documentation
- Ensure Sponsors confirm legitimate need for Third Party engagement
- Provide Compliance Department oversight for Medium, High, and Very High Risk Third Parties
- Protect **Digital Edge**s' reputation by only engaging reputable third parties
- Minimize risks associated with Third Party relationships
- Prevent involvement in corrupt activities or with corrupt actors
- Demonstrate credible due diligence, decision making, contracting, and monitoring
- Support non-retaliation **Policy** for good faith reporting of violations

Before entering a relationship or renewing an existing relationship with a Third Party, a Sponsor must comply with requirements of this Policy. Violations of this Policy will result in disciplinary action by Digital Edge, which may include termination of the Sponsor's employment with Digital Edge, and the termination of Digital Edge's engagement with the Third Party.

DOs AND DON'Ts

DOs

DO comply with all requirements of Third Party Due Diligence **Policy** and Procedures before entering or renewing any Third Party relationship

DO understand that third parties are essential to **Digital Edge** success and reflect who **Digital Edge** is

DO ensure you only deal with third parties who are reputable and prepared to apply same standards of business conduct

DO carefully vet all third parties before engaging with them

DO understand that **Digital Edge** can be held accountable for actions of those acting on **Digital Edge** behalf

DO promote compliance with Business Code of Conduct, Trade Sanctions **Policy**, Anti-Money Laundering, Anti-Bribery Anti-Corruption **Policy**, and applicable laws

DO register all Third Parties in Third-Party GAN Integrity Due Diligence Platform (Platform) before engagement

DO classify Third Parties correctly as Level 1 (engaging with others on **Digital Edge** behalf) or Level 2 (dealing only with **Digital Edge**)

DO contact Legal / Compliance Department if you have any doubt about classification of Third Party

DO complete Internal Questionnaire truthfully and fully for all Level 1 Third Parties

DO assign initial Risk Rating as Very Low, Low, Medium, High, or Very High Risk

DO conduct appropriate level of due diligence based on Risk Rating (Basic, Mid-Level, or Enhanced)

DO conduct Vantage Screening including negative Internet searches and database checks

DO send Third-Party Due Diligence Questionnaire to Medium, High, and Very High Risk Third Parties via Platform

DO escalate all Red Flags to Legal / Compliance Department for further consideration

DO ensure all Red Flags are resolved or mitigated before moving to final approval process

DO document mitigation and monitoring measures for unresolved Red Flags in Platform

DO complete Final Evaluation certifying appropriate due diligence has been completed

DO enter into written Agreement with Third Party before engagement and payment

DO include mandatory compliance clauses in all Agreements (anti-bribery statements, compliance with ABC Laws, no sub-contracting without consent, no assignment without consent, Material Change notification, termination rights)

DO include additional clauses for High Risk Third Parties (right to audit, annual Compliance Confirmation, ABC training requirements)

DO incorporate **Digital Edge** Business Partner Code of Conduct into Agreements

DO monitor Third Parties continuously through Vantage Screening tool in Platform

DO notify Legal / Compliance Department immediately of any new Red Flags or concerns about Third Party integrity

DO assess impact of Material Changes or newly identified Red Flags on decision to continue engagement

DO ensure timely renewal of due diligence at required intervals (4 years for Very Low/Low Risk, 3 years for Medium Risk, 1 year for High/Very High Risk)

DO obtain annual Compliance Confirmation from High, Very High Risk, and some Medium Risk Third Parties

DO maintain completed and updated due diligence file on each Third Party in Platform

DO upload all documentation to Platform for proper record keeping

DO send copies of documents to Compliance Department for storage per Records Management **Policy**

DO confirm legitimate need for goods or services provided by Third Party

DO ensure payments to Third Party are consistent with service delivery and Agreement terms

DO complete mitigation measures assigned to you within allocated timeframes

DO cooperate with Legal / Compliance Department in all Medium, High, and Very High Risk Third Party due diligence

DO understand timelines for due diligence (less than 1 day for Very Low/Low Risk, 5 business days for Medium/High/Very High Risk, 3-4 weeks for Enhanced Due Diligence)

DO understand costs for Enhanced Due Diligence borne by business unit requesting engagement

DO report violations or concerns to Chief Legal Officer or Compliance Department

DO use non-retaliation protections when reporting violations or raising compliance concerns in good faith

DO contact Chief Legal Officer (joe.b@digitaledgedc.com) or Compliance Department (vishal.jain@digitaledgedc.com) if you have questions

DON'Ts

DON'T enter or renew Third Party relationship without complying with **Policy** requirements

DON'T engage third parties who are not reputable or not prepared to apply same standards of business conduct

DON'T fail to carefully vet third parties before engaging with them

DON'T ignore that **Digital Edge** can be held accountable for actions of those acting on **Digital Edge** behalf

DON'T skip or inadequately perform required due diligence based on Risk Rating

DON'T fail to send Third-Party Due Diligence Questionnaire to Medium, High, and Very High Risk Third Parties

DON'T proceed to final approval if Red Flags remain unresolved and not mitigated

DON'T fail to document mitigation and monitoring measures in Platform

DON'T fail to properly complete Final Evaluation

DON'T engage Third Party without approval in Platform

DON'T fail to include mandatory compliance clauses in Agreements

DON'T fail to include additional clauses for High Risk Third Parties (audit rights, Compliance Confirmation, training)

DON'T allow Third Party to begin work before due diligence complete, approval obtained, and Agreement executed

DON'T ignore new Red Flags or concerns about Third Party integrity

DON'T fail to notify Legal / Compliance Department of Material Changes or new Red Flags

DON'T fail to assess impact of changes on decision to continue engagement

DON'T use outdated due diligence (older than 3 years for Very Low/Low Risk, 2 years for Medium Risk, 1 year for High/Very High Risk) when renewing Agreements

DON'T fail to renew due diligence at required intervals

DON'T fail to obtain annual Compliance Confirmation from High and Very High Risk Third Parties

DON'T fail to maintain completed due diligence files in Platform

DON'T fail to upload documentation to Platform

DON'T fail to send copies to Compliance Department for proper storage

DON'T engage Third Party without confirming legitimate need for goods or services

DON'T make payments inconsistent with service delivery or Agreement terms

DON'T fail to complete assigned mitigation measures within timeframes

DON'T fail to cooperate with Legal / Compliance Department in due diligence process

DON'T underestimate timelines required for proper due diligence

DON'T engage Third Party Rejected in Platform

DON'T allow assignment of Agreement without **Digital Edge** prior written consent

DON'T fear retaliation when reporting violations or raising compliance concerns in good faith (**Digital Edge** committed to non-retaliation)

DON'T fail to report violations or concerns about Third Party compliance

DON'T hesitate to contact Chief Legal Officer or Compliance Department if you have questions about **Policy**

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What is the scope and purpose of this Policy?

A: This **Policy** applies to **Digital Edge** worldwide operations and all **Digital Edge** Personnel. The objective is to ensure appropriate due diligence is undertaken on all Third Parties before engagement to promote compliance with **Digital Edge Policies** and applicable laws, including Business Code of Conduct, Trade Sanctions **Policy**, Anti-Money Laundering, and Anti-Bribery Anti-Corruption **Policy**. Before entering or renewing any Third Party relationship, a Sponsor must comply with **Policy** requirements. Violations result in disciplinary action up to termination of employment and termination of Third Party engagement.

Q2: What is the difference between Level 1 and Level 2 Third Parties?

A: Level 1 Third Parties engage directly or indirectly with others (customs officials, government officials, end-users) on **Digital Edge** behalf. Examples include joint venture partners, suppliers/vendors dealing with third parties, agents, service providers with third party obligations, advisers/intermediaries representing **Digital Edge**, resellers/wholesalers, contractors/sub-contractors, M&A targets, and consultants. Level 2 Third Parties deal only with **Digital Edge** without third party interactions. Examples include suppliers/vendors without third party obligations, service providers without third party obligations, advisers working directly for **Digital Edge**, and customers (end-users).

Q3: How are Third Parties classified by Risk Rating?

A: Risk Ratings are Very Low, Low, Medium, High, or Very High Risk. Level 2 Third Parties are presumed to be Low Risk unless Vantage Screening discovers unresolved Red Flags. Level 1 Third Parties receive Risk Rating after Sponsor completes Internal Questionnaire asking questions about common Risk Indicators. JV Partners and M&A Targets automatically classified High Risk. Risk Rating determines due diligence level required (Basic, Mid-Level, or Enhanced) and level of approval authority needed.

Q4: What is the seven-step Third Party on-boarding process?

A: Step 1: Registration and Pre-Classification in Platform; Step 2: Risk Assessment (Very Low to Very High Risk); Step 3: Due Diligence (Vantage Screening, questionnaires, investigations); Step 4: Decision-Making/Final Evaluation and approval; Step 5: Post-Approval Contracting with mandatory compliance clauses; Step 6: Monitoring (continuous Vantage Screening and event-triggered activities);

Step 7: Record Keeping and documentation in Platform. Process largely automated through Platform with Legal Department involvement for Medium, High, and Very High Risk Third Parties.

Q5: What are Red Flags and how are they handled?

A: Red Flags are information indicating increased corruption risk or potential issues with Third Party ownership, business structure, relationships, or legal compliance. Common Red Flags include ties to government, questionable circumstances, unusual compensation requests, poor reputation, insufficient capabilities, and potential sanctions issues. All Red Flags must be escalated to the Compliance Department. Red Flags must be resolved or mitigated before final approval. Mitigation and monitoring measures must be documented in Platform and assigned for completion.

Q6: What are the mandatory contracting requirements?

A: Third Party can only be engaged if approved in Platform and written Agreement executed. Agreements must include: description of services and remuneration; anti-bribery statement (no bribes, grounds for termination); compliance with ABC Laws (FCPA, UK Bribery Act); no sub-contracting without prior written consent from the Chief Legal Officer; no assignment without prior consent; Material Change notification obligation; termination rights for breaches, omissions/misrepresentations, and delays in Compliance Confirmation. High Risk Third Parties require additional clauses: audit rights, annual Compliance Confirmation, and ABC training for personnel.

Q7: What are the monitoring and renewal requirements?

A: All approved Third Parties continuously monitored through Vantage Screening tool. Sponsors and the Compliance Department notified of new Red Flags. Sponsors must monitor for compliance concerns and notify the Legal / Compliance Department immediately. Due diligence must be renewed: every 4 years for Very Low/Low Risk Third Parties; every 3 years for Medium Risk Third Parties; every 1 year for High/Very High Risk Third Parties. High and Very High Risk Third Parties must provide annual Compliance Confirmation. Sponsors must update Platform when Material Changes or new Red Flags are identified.

Q8: What are Sponsor responsibilities?

A: Sponsors have ultimate responsibility for managing Third Party risks. Responsibilities include: confirming legitimate need for goods/services; classifying Third Party as Level 1 or Level 2; completing Internal Questionnaire truthfully for Level 1 Third Parties; performing Low-risk Basic Due Diligence; sending questionnaires to Medium/High/Very High Risk Third Parties; ensuring Legal Department has necessary information; completing Final Evaluation for Low-risk Third Parties; ensuring approvals before engagement; ensuring Third Party does not begin work until complete; maintaining updated files and uploading to Platform; monitoring Third Party and ensuring payments consistent with Agreement; completing mitigation measures; performing subsequent assessments as required. A Sponsor should be at the level of E-3 and above to ensure appropriate seniority in respect of the engagement and management of the Third-Party relationship.

Q9: What are Legal Department responsibilities?

A: Legal Department performs all Medium, High, and Very High Risk Third Party due diligence (or ensures qualified vendor performs it); prepares Final Evaluation for Medium, High, and Very High Risk Third Parties; supports Sponsors in making informed decisions; monitors and performs subsequent assessments; reviews key suppliers; conducts ad-hoc reviews when Red Flags identified; may engage external vendors (e.g., Control Risks) for Enhanced Due Diligence; reclassifies Risk Ratings when appropriate; ensures Red Flags resolved or mitigated; provides guidance on classification and compliance.

Q10: How long does the due diligence process take and who do I contact with questions?

A: Very Low to Low Risk Third Party due diligence typically takes less than 1 day. Medium, High, and Very High Risk due diligence normally takes 5 business days upon receipt of required documentation. Enhanced Due Diligence takes 3-4 weeks. Costs for Enhanced Due Diligence charged to relevant business unit requesting engagement. Longer times are expected if Red Flags are identified. Contact Chief Legal Officer or Compliance Department. **Digital Edge** committed to non-retaliation for good faith reporting.

SEVEN-STEP THIRD PARTY ON-BOARDING PROCESS

The on-boarding and management of Third Parties follows systematic seven-step process:

1. **Step 1: Third Party Registration and Pre-Classification**

    - Sponsor registers Third Party in Platform
    - Input full legal name, registered address, location, type of proposed engagement
    - Classify as Level 1 (engaging with others on **Digital Edge** behalf) or Level 2 (dealing only with **Digital Edge**)
    - Contact Legal Department if doubt about classification
    - Platform automatically selects appropriate workflow

2. **Step 2: Risk Assessment**

    - Sponsor and Legal Department classify initial Risk Rating: Very Low, Low, Medium, High, Very High
    - Level 2 Third Parties presumed Low Risk unless Vantage Screening discovers Red Flags
    - Level 1 Third Parties receive Risk Rating after Internal Questionnaire completed
    - Internal Questionnaire asks about common Risk Indicators
    - Platform assigns Risk Rating and pre-selects workflow based on responses
    - Risk Rating determines due diligence level and approval authority required

3. **Step 3: Due Diligence**

   - Very Low/Low Risk: Platform conducts automated Vantage Screening (negative Internet searches and database checks)
   - Medium Risk: All Low Risk activities plus Third-Party Due Diligence Questionnaire, research Key Individuals, adverse searches, verify references
   - High/Very High Risk: All Medium Risk activities plus local public database searches, Politically Exposed Persons screening, enhanced investigation
   - Legal Department determines if Enhanced Due Diligence required (may engage Control Risks or external vendors)
   - All Red Flags escalated to Legal Department for review
   - Red Flags must be resolved or mitigated before approval

4. **Step 4: Decision-Making and Final Evaluation**

   - Results documented in Platform with recommendation to proceed or not
   - Very Low/Low Risk: Sponsor completes Final Evaluation and approves/rejects
   - Medium/High/Very High Risk: Legal Department completes Final Evaluation in consultation with Sponsor
   - Final Evaluation certifies: type and risk classification; appropriate due diligence completed; Red Flags resolved or mitigated; mitigation measures documented
   - Sponsor can only proceed if Third Party Approved in Platform
   - Third Party Rejected in Platform shall not be engaged

5. **Step 5: Post-Approval Process and Contracting**

   - Third Party can only be engaged if approved in Platform AND written Agreement executed
   - Agreement must describe services/products and remuneration terms
   - Mandatory clauses: anti-bribery statement, compliance with ABC Laws, no sub-contracting without consent, no assignment without consent, Material Change notification, termination rights
   - High Risk additional clauses: audit rights, annual Compliance Confirmation, ABC training requirements
   - Incorporate Business Partner Code of Conduct into Agreement
   - Any deviation requires Chief Legal and Compliance Officer approval

6. **Step 6: Monitoring**

   - Continuous monitoring through Vantage Screening tool in Platform
   - Sponsor and Legal Department notified of new Red Flags
   - Sponsor monitors for compliance concerns and notifies Legal Department
   - Event-Triggered Monitoring: assess impact of Material Changes or new Red Flags on decision to continue engagement
   - Renewal of Due Diligence: 4 years (Very Low/Low Risk), 3 years (Medium Risk), 1 year (High/Very High Risk)

- Pre-Defined Monitoring: High/Very High Risk Third Parties provide annual Compliance Confirmation
- Update Platform when circumstances change

7. **Step 7: Record Keeping**

- Upload and retain all documentation in Platform
- Demonstrates reasonable precautions to avoid corrupt activities or actors
- Evidence of credible due diligence, decision making, contracting, monitoring
- Send copies to Legal Department for storage per Records Management **Policy**
- Maintain completed and updated due diligence file for each Third Party

---

THIRD PARTY CATEGORIES

Level 1 Third Parties (Engaging with Others on Digital Edge Behalf)

Definition: Third Party likely to engage directly or indirectly with another party (customs officials, government officials, end-users, other third parties) on **Digital Edge**'s behalf or in connection with contractual duties being performed for **Digital Edge**.

Classification Questions:

- Will Third Party perform services on behalf of **Digital Edge** or be authorized to represent **Digital Edge** vis-à-vis other third parties?
- Is it reasonable to expect that Third Party will come into contact with government officials when representing or performing services on behalf of **Digital Edge**?
- Will Third Party be able to influence the decisions or conduct of unrelated third parties for the benefit of **Digital Edge**?

A positive response to any of the classification questions will result in a Level 1 classification being applied and a more detailed review will be required.

Examples:

- **Joint Venture Partner:** Individual/organization entering business agreement to establish new business entity. Automatically classified High Risk.
- **Supplier/Vendor:** Supplies parts/services and has a contractual obligation to deal with third parties on **Digital Edge**'s behalf (import agents, customs, permits, authorizations).
- **Agent:** Authorized to act for or represent **Digital Edge** in furtherance of business interests. Types: Sales agents (winning contracts), Process agents (importer, permits, licenses).
- **Service Provider:** Provides functional support (communications, logistics, storage, processing) and has a contractual obligation to deal with third parties on **Digital Edge**'s behalf.
- **Adviser and Intermediaries:** Provides service/advice by representing **Digital Edge** towards another person, business, and/or government official (legal, tax, financial,

consultant, lobbyist). Note: excludes advisors providing typical due diligence/transaction advisory work directly to **Digital Edge**.

- **Reseller/Wholesaler:** Buys products from **Digital Edge** and resells directly to end-users.
- **Contractor and Sub-contractor:** Non-controlled individual/organization providing goods/services under contract. Sub-contractor hired by contractor for a specific task.
- **M&A Targets:** Targets of acquisitions or mergers. Includes shareholders (sellers of target). Automatically classified High Risk.
- **Consultant:** Entity/individual engaged on an exclusive or non-exclusive basis to perform services on **Digital Edge** behalf (sales consultant, business development consultant).

Level 2 Third Parties (Dealing Only with Digital Edge)

Definition: Third Party who deals only with **Digital Edge** in performance of contractual duties without third party interactions.

Examples:

- **Supplier/Vendor:** Supplies parts/services without the need for consent or authorization from third parties (customs officials, government officials).
- **Service Provider:** Provides functional support without the need for consent or authorization from third parties.
- **Adviser and Intermediaries:** Provides service/advice to **Digital Edge** only (not towards or acting with another person, business, and/or government official). Legal, tax, financial, business consultant.
- **Customer:** Ultimate customer of products and services (end-user).

DUE DILIGENCE LEVELS

Basic Due Diligence (Very Low/Low Risk)

Level 1 Third Parties:

- Verification of Third Party business information (address, Company name, registration number)
- Complete Internal Questionnaire by Sponsor
- Conduct Vantage Screening (automated)

Level 2 Third Parties:

- Verification of Third Party business information
- Conduct Vantage Screening (automated)

Mid-Level Due Diligence (Medium Risk)

All Level 1 or Level 2 Low Risk activities PLUS:

- Third Party completes Due Diligence Questionnaire

- Research Key Individuals (management, board members, significant shareholders)
- Conduct adverse internet and media searches of Key Individuals in local languages and/or English
- Verification of references collected in Questionnaire

Enhanced Due Diligence (High/Very High Risk)

All Medium Risk activities PLUS:

- Local public database searches focusing on in-country public records (litigation, regulatory, criminal, bankruptcy, directorship roles) of Third Party and Key Individuals
- Screening of Third Party and Key Individuals against Politically Exposed Persons List
- Verification of references collected in Questionnaire
- Legal Department may use external vendors (e.g., Control Risks) for activities
- Costs borne by business unit requesting engagement
- Takes 3-4 weeks to complete

KEY RISK INDICATORS

Broad contextual factors making bribery or corruption more likely to occur:

Geographic Location

- Country with Corruption Perception Index score of 50 or below (see Transparency International's Corruption Perceptions Index)
- Jurisdiction with high levels of bank secrecy and high risk for facilitating illicit financial flows (see Tax Justice Network's Financial Secrecy Index)
- Jurisdiction encouraging or requiring hiring local agents to transact business with government

Industry

- Industry perceived to present high risk for corruption (see Transparency International's Bribe Payers Index)
- Industry with history of anti-corruption enforcement scrutiny (oil & gas, logistics, mineral extraction, construction)

Background and Identity of Third Party

- Initial Internet searches reveal significant problems related to reputation for integrity
- Third Party or senior officials previously subject to regulatory action or legal proceedings for alleged ABC Laws breaches
- Third Party or senior officials appear on denied parties/persons list due to sanctions or past misconduct
- Third Party has little or no experience in relevant industry sector and/or unknown to organization

Connection with Government Officials or Entities

- Third Party will have frequent interaction with government officials (customs officials, governmental agencies, government-controlled entities) while doing work for **Digital Edge**
- Third Party wholly or partly (directly or indirectly) owned by government official/entity or has links with government officials/entities
- Third Party previously worked for government or closely connected with political elite

Compensation Structure

- Compensation based on performance (success fees, bonus fees, contingency fees)
- Payment required by unusual means (deviating from standard practice, multiple accounts, upfront payments, split into small amounts, in cash, in country/currency different from domicile or work location)
- Compensation takes form of political or charitable contribution

Scope of Services

- Third Party role is to enhance organization's chances of winning commercial and/or government contracts
- Third Party requests discretionary authority to handle local matters alone

Selection of Third Party

- Third Party recommended by customer
- Retention of specific Third Party encouraged or required by government official

---

COMMON RED FLAGS

Information indicating increased corruption risk or potential issues:

Ties to Government

- Family or business ties to government officials or employees
- Large or frequent political contributions
- Government official or employee recommended Third Party
- References to political or charitable donations as a way to influence official actions or outcomes
- Large sales to government agencies with unusually high unit price and low frequency

Questionable Circumstances

- Refusal to cooperate with due diligence or refusal to make representations and warranties in Agreement
- Third Party not in compliance with local law

- Suspicious statements (needing money to "get the business" or "make necessary arrangements")
- Submitting invoices or requests payment with suspicious entries or under suspicious circumstances
- Bankruptcies, default on obligations, civil suits alleging fraud, property seizures, criminal or regulatory issues

Unusual Compensation

- Requesting commission or payment substantially above market rate or substantial up-front payment
- Requesting payments in cash or in checks payable to cash or bearer
- Requesting payment through third party or in third country
- Refusal or inability to properly document expenses

Poor Reputation

- Reputation for unethical conduct
- Country where Third Party based or where business will be conducted has reputation for corruption

Insufficient Capabilities

- Third Party not expected to perform substantial work
- Third Party lacks staff, facilities, or expertise to perform substantial work
- Third Party lacks relevant industry/technical experience

Potential Sanctions Issues

- Third Party identity not clear
- Third Party usually involved in military related business
- Third Party or address similar to party on OFAC sanctioned entity list
- Purchasing agent reluctant to offer information about end-use of goods

---

ROLES AND RESPONSIBILITIES

Sponsor Responsibilities

Sponsor has ultimate responsibility for managing and mitigating Third Party risks:

- Confirm legitimate need for goods and/or service provided by Third Party
- Make assessment as to category of Third Party (Level 1 or Level 2)
- Answer Internal Questionnaire for all Level 1 Third Parties as truthfully and fully as possible
- Perform all Low-risk Basic Due Diligence and notify Legal Department of potential Red Flags

- Prepare and send Third-Party Due Diligence Questionnaire to all Medium, High, Very High Risk Third Parties via Platform
- Ensure Legal Department provided with all necessary information to fulfill **Policy** requirements
- Prepare and complete Final Evaluation for all Low-risk Third Parties
- Ensure all approvals received prior to engaging Third Party
- Ensure Third Party does not begin work until due diligence complete, Third Party approved in Platform, and Agreement executed
- Keep completed and updated due diligence file on each Third Party and upload to Platform
- Send documents received outside Platform to Legal Department for review and proper storage
- Monitor Third Party in adherence to Agreement and ensure payments consistent with service delivery and Agreement terms
- Ensure mitigation measures assigned to Sponsor completed within allocated timeframes
- Perform monitoring and subsequent assessments after Third Party engaged as required by **Policy**

Legal Department Responsibilities

- Perform all Medium, High, Very High Risk Third Party due diligence or ensure performed by qualified third-party vendor
- Prepare Final Evaluation for all Medium, High, Very High Risk Third Parties
- Support Sponsor and other parties in making informed decision about Third Party engagement
- Monitor and perform subsequent assessments after Third Party engaged as required by **Policy**
- Reclassify Risk Ratings when appropriate based on Vantage Screening or other information
- Determine if Enhanced Due Diligence required and engage external vendors (e.g., Control Risks)
- Review and resolve Red Flags before final approval
- Document mitigation and monitoring measures in Platform
- Provide guidance on Third Party classification and **Policy** compliance
- Store documentation

MONITORING REQUIREMENTS

Continuous Monitoring

- All approved Third Parties continuously monitored via Vantage Screening tool in Platform
- Sponsor and Legal Department notified of any new Red Flag identified
- Sponsor must continually monitor Third Party to detect compliance concerns
- Notify Legal Department as soon as reasonably practicable of concerns

Event-Triggered Monitoring Activities

- When change in circumstances (Material Change to structure or newly identified Red Flags)
- Assess impact on decision to continue engaging Third Party
- Determine possible mitigating and monitoring measures
- Update Third Party due diligence file in Platform accordingly
- Sponsor must inform Legal Department of relevant information affecting risk classification

Renewal of Due Diligence

Due diligence process must be renewed at least once every:

- 4 years for Very Low and Low Risk Third Parties
- 3 years for Medium Risk Third Parties
- 1 year for High and Very High Risk Third Parties

Platform notifies Sponsor and Legal Department when time to renew.

Prior to renewing Agreement, ensure due diligence not older than:

- 3 years for Very Low or Low Risk Third Parties
- 2 years for Medium Risk Third Parties
- 1 year for High or Very High Risk Third Parties

Otherwise, new due diligence required even if Agreement contains auto-renewal clause.

Pre-Defined Monitoring Activities

- High, Very High Risk, and some Medium Risk Third Parties (as determined by Legal Department) provide annual Compliance Confirmation
- Sponsor responsible for obtaining Compliance Confirmation and uploading to Platform

REPORTING AND NON-RETALIATION

Reporting Obligations

You have an obligation to Digital Edge and colleagues to help maintain high ethical business standards.

Contact:

- Chief Legal Officer: joe.b@digitaledgedc.com
- Compliance Department: vishal.jain@digitaledgedc.com

Non-Retaliation Commitment

Digital Edge is committed to non-retaliation.

- **Digital Edge** will not impose sanctions or permit retribution against person who promptly reports information of violations or participates in investigation of suspected violation (and who has not engaged in such conduct)
- Any employee who reports potential violation or raises compliance concern in good faith is doing right thing and may do so without fear of retaliation
- **Digital Edge** will take prompt disciplinary action against any employee who retaliates against you, up to and including termination of employment

REMEMBER

Third parties are essential to Digital Edge success and reflect who we are as a Company. We must only deal with third parties who are reputable and prepared to apply the same standards of business conduct as we do ourselves. Before entering or renewing any Third Party relationship, you must comply with all requirements of the Third Party Due Diligence Policy and Procedures. Register all Third Parties in the Platform, classify correctly as Level 1 or Level 2, complete Internal Questionnaire truthfully for Level 1 Third Parties, assign appropriate Risk Rating (Very Low, Low, Medium, High, Very High), conduct required due diligence (Basic, Mid-Level, or Enhanced), escalate all Red Flags to Legal Department, ensure Red Flags are resolved or mitigated, complete Final Evaluation, obtain approval in Platform before engagement, execute written Agreement with mandatory compliance clauses, monitor continuously through Platform, renew due diligence at required intervals (4 years for Very Low/Low Risk, 3 years for Medium Risk, 1 year for High/Very High Risk), and maintain proper documentation in Platform. Do not allow Third Party to begin work until due diligence complete, approval obtained, and Agreement executed. Violations of Policy result in disciplinary action up to termination of employment and termination of Third Party engagement. If you have questions or concerns, contact the Compliance Department. Digital Edge is committed to non-retaliation for good faith reporting of violations or compliance concerns.

ANTI-HUMAN TRAFFICKING AND ANTI-MODERN SLAVERY STATEMENT

This section provides a high-level overview of Digital Edge's Anti-Human Trafficking and Anti-Modern Slavery Statement for ease of reference. Employees should refer to the detailed Anti-Human Trafficking and Anti-Modern Slavery Statement Anti-Human Trafficking and Anti-Modern Slavery Statement available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

The Anti-Human Trafficking and Anti-Modern Slavery Statement ("**Statement**") sets forth **Digital Edge** commitment to combating human trafficking and modern slavery and clearly communicates the ethical conduct expected from all stake holders including but not limited to directors, officers, employees, and third-party business partners.

Human trafficking and modern slavery are violations of fundamental human rights. Though there are many manifestations, they are all intended to exploit vulnerable persons for the gratification or commercial gain of others. **Digital Edge** is committed to ensuring that human trafficking and modern slavery never play a part in our workplace or in our supply chain.

Key Principles:

- Human trafficking and modern slavery are violations of fundamental human rights
- **Digital Edge** has zero-tolerance **Policy** for any instances of human trafficking or modern slavery
- Same opposition demanded from all who work for or with **Digital Edge**
- Though not currently subject to UK Modern Slavery Act of 2015 or Australian Modern Slavery Act of 2018, **Digital Edge** believes it is best practice to address modern slavery risks
- **Digital Edge** uses all available tools to avoid human trafficking and modern slavery (Governance Programs, Code of Conduct, Business Partner Code of Conduct, Third Party Due Diligence **Policy**, Whistleblower **Policy**, contracting terms, training programs)
- **Digital Edge** carries out risk-based due diligence on all third parties
- Third Party Due Diligence **Policy** promotes compliance with **Digital Edge Policies** and applicable laws
- **Digital Edge** assesses potential human rights risks of supply chains by considering origin of suppliers and monitoring their approach to modern slavery
- Risk is particularly high when any unskilled, temporary, or outsourced labor is involved
- **Digital Edge** regularly assesses supply chain to determine if any element is higher risk
- Key suppliers reviewed more frequently by Legal Department and, if required, external advisors

- Reviews and investigations may be conducted on ad-hoc basis if issues raised by whistleblowers or on ethics and compliance hotline
- Code of Conduct and Business Partner Code of Conduct set forth expectations of ethical conduct
- Adherence to Codes is pre-condition to continued association with **Digital Edge**
- Employees and business partners undergo periodic training to ensure compliance
- Annual trainings provided live and online in multiple languages
- Employees required to certify compliance with and recommit to Code on annual basis
- Whistleblower **Policy** and helpline available to address questions or concerns
- Zero tolerance, non-retaliation **Policy** protects employees when they raise concerns

---

STATEMENT OBJECTIVE

The purpose of this Statement is to reflect **Digital Edge**'s determination to ensure that human trafficking and modern slavery play no part in the conduct of our business or in our supply chain.

The Statement is designed to:

- Establish **Digital Edge**'s commitment to combating human trafficking and modern slavery
- Communicate ethical conduct expected from employees and business partners
- Apply **Digital Edge**'s worldwide operations to anti-human trafficking and anti-modern slavery standards
- Establish zero-tolerance policy for any instances of human trafficking or modern slavery
- Address modern slavery risks in business and supply chain as best practice
- Utilize all available tools to avoid human trafficking and modern slavery (Governance Programs, Codes of Conduct, Due Diligence **Policies**, Whistleblower **Policy**, contracting terms, training)
- Ensure **Digital Edge** only deals with third parties who are reputable and prepared to abide by same standards of business conduct
- Promote compliance by **Digital Edge** and third-party business partners with **Digital Edge Policies** and applicable laws
- Minimize risks associated with engaging and working with Third Parties
- Assess potential human rights risks of supply chains by considering origin of suppliers and monitoring their approach to modern slavery
- Identify and manage risks particularly high when unskilled, temporary, or outsourced labor is involved
- Conduct regular supply chain assessments and physical inspections when risk assessment determines it to be sensible
- Review key suppliers more frequently by Legal / Compliance Department and external advisors
- Conduct ad-hoc reviews and investigations when issues raised by whistleblowers or ethics hotline
- Set forth expectations of ethical conduct through publicly available Codes
- Require adherence to Codes as pre-condition to continued association with **Digital Edge**

- Provide periodic training to employees and business partners to ensure compliance with Codes
- Require employees to certify compliance with and recommit to Code on annual basis
- Protect employees through zero tolerance, non-retaliation **Policy** when they raise concerns

Although Digital Edge is not currently subject to the UK Modern Slavery Act of 2015 or the Australian Modern Slavery Act of 2018, Digital Edge believes it is best practice to address modern slavery risks in our business and supply chain.

DOs AND DON'Ts

DOs

DO comply with all applicable laws, rules, and regulations relating to human trafficking and modern slavery

DO follow all internal **Digital Edge Policies** including Code of Conduct, Business Partner Code of Conduct, Third Party Due Diligence **Policy**, and Whistleblower **Policy**

DO observe the highest ethical standards in the conduct of your duties and responsibilities

DO understand that human trafficking and modern slavery are violations of fundamental human rights

DO be aware that human trafficking and modern slavery are intended to exploit vulnerable persons for gratification or commercial gain of others

DO ensure that human trafficking and modern slavery never play a part in your work for **Digital Edge** or in interactions with supply chain

DO adhere to **Digital Edge**'s zero-tolerance **Policy** for any instances of human trafficking or modern slavery

DO demand the same opposition to human trafficking and modern slavery from all who work for or with you

DO understand **Digital Edge** uses all available tools to avoid human trafficking and modern slavery

DO ensure you only deal with third parties who are reputable and prepared to abide by same standards of business conduct

DO comply with Third Party Due Diligence **Policy** and Procedures when engaging third parties

DO promote compliance by third-party business partners with **Digital Edge**'s **Policies** including Code of Conduct, Business Partner Code of Conduct, Trade Sanctions **Policy**, Anti-Money Laundering, Anti-Bribery Anti-Corruption **Policy**, and this Statement

DO minimize risks associated with engaging and working with Third Parties

DO assess potential human rights risks of supply chains by considering origin of suppliers

DO understand and monitor suppliers' approach to modern slavery as part of supplier on-boarding process

DO actively engage with direct suppliers and thoroughly scrutinize their management systems as it relates to their upstream suppliers

DO be particularly vigilant when any unskilled, temporary, or outsourced labor is involved

DO regularly assess supply chain to determine whether any element may be of higher risk than previously assessed

DO support physical inspections when risk assessment determines it to be sensible

DO ensure evaluation starts when supplier is on-boarded to help identify any high-risk suppliers

DO subject suppliers to on-going assessment process against range of criteria including compliance with ethical standards and corporate values

DO cooperate with Legal / Compliance Department in reviewing key suppliers more frequently

DO cooperate with ad-hoc reviews and investigations, particularly if issues are raised by whistleblowers or on ethics and compliance hotline

DO read and comply with Code of Conduct and Business Partner Code of Conduct which are publicly available on **Digital Edge**'s website

DO understand adherence to these Codes is pre-condition to continued association with **Digital Edge**

DO ensure human trafficking and modern slavery are never a part of **Digital Edge**'s supply chain or workplace

DO undergo periodic training to ensure compliance with Codes

DO attend annual trainings provided live and online (available in multiple languages)

DO use Whistleblower **Policy** and helpline to address questions or concerns related to Codes

DO understand **Digital Edge** enforces zero tolerance, non-retaliation **Policy** that protects employees when they raise concerns

DO raise concerns about suspected human trafficking or modern slavery without fear of retaliation

DON'Ts

DON'T tolerate or participate in human trafficking or modern slavery in any form

DON'T exploit vulnerable persons for gratification or commercial gain

DON'T allow human trafficking or modern slavery to play any part in your work for **Digital Edge** or in interactions with supply chain

DON'T work with individuals or entities who tolerate human trafficking or modern slavery

DON'T engage third parties without carrying out risk-based due diligence

DON'T deal with third parties who are not reputable or not prepared to abide by same standards of business conduct

DON'T fail to promote compliance by third-party business partners with **Digital Edge**'s **Policies** and applicable laws

DON'T neglect to assess potential human rights risks of supply chains

DON'T fail to consider origin of suppliers when assessing modern slavery risks

DON'T fail to understand and monitor suppliers' approach to modern slavery during on-boarding process

DON'T fail to engage with direct suppliers or scrutinize their management systems regarding upstream suppliers

DON'T overlook risks when unskilled, temporary, or outsourced labor is involved

DON'T fail to evaluate suppliers when they are on-boarded to identify high-risk suppliers

DON'T fail to subject suppliers to on-going assessment process

DON'T fail to cooperate with Legal / Compliance Department in reviewing key suppliers

DON'T fail to cooperate with ad-hoc reviews and investigations when issues are raised

DON'T fail to read and comply with Code of Conduct and Business Partner Code of Conduct

DON'T continue association with **Digital Edge** if you fail to adhere to Codes (adherence is pre-condition)

DON'T allow human trafficking or modern slavery to be part of **Digital Edge**'s supply chain or workplace

DON'T fail to attend annual trainings provided by **Digital Edge**

DON'T fail to certify compliance with and recommit to Code on annual basis

DON'T fail to use Whistleblower **Policy** and helpline when you have questions or concerns

DON'T fear retaliation when raising concerns (**Digital Edge** enforces zero tolerance, non-retaliation **Policy**)

DON'T hesitate to contact **Policy** Representative if you have questions about this Statement or any situation or concern

---

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What is the scope of this Statement and who must comply?

A: This Statement is applicable to **Digital Edge**'s worldwide operations. This Statement sets forth **Digital Edge**'s commitment to combating human trafficking and modern slavery and clearly communicates the ethical conduct we expect from our employees (including our contingent workers, agents, contractors, and consultants providing services on behalf of **Digital Edge**) as well as from all our business partners. **Digital Edge** expects its directors, officers, employees, and third-party business partners to comply with all applicable laws, rules, and regulations and to follow all internal **Digital Edge Policies**, observing the highest ethical standards in the conduct of their duties and responsibilities.

Q2: What are human trafficking and modern slavery?

A: Human trafficking and modern slavery are violations of fundamental human rights. Though there are many manifestations, they are all intended to exploit vulnerable persons for the gratification or commercial gain of others. **Digital Edge** is committed to ensuring that human trafficking and modern slavery never play a part in our workplace or in our supply chain.

Q3: What is Digital Edge's Policy regarding human trafficking and modern slavery?

A: **Digital Edge** has a zero-tolerance **Policy** for any instances of human trafficking or modern slavery, and we demand the same opposition from all who work for or with us. **Digital Edge** will use all available tools to avoid human trafficking and modern slavery. Though **Digital Edge** is not currently subject to the UK Modern Slavery Act of 2015 or the Australian Modern Slavery Act of 2018, **Digital Edge** believes it is best practice to address modern slavery risks in our business and supply chain.

Q4: How does Digital Edge ensure it only deals with reputable third parties?

A: **Digital Edge** recognizes that its business partners reflect **Digital Edge** 's identity and are essential to its success. Consequently, the Company carries out risk-based due diligence on all third parties to promote compliance with ethical standards and minimize the risks associated with external engagements. The objective of our Third Party Due Diligence **Policy** and Procedures is to promote compliance by **Digital Edge** and our third-party business partners (Third Parties or Third Party) with **Digital Edge**'s various **Policies**, including our Code of Conduct, Business Partner Code of Conduct, Trade Sanctions **Policy**, Anti-Money Laundering, Anti-Bribery Anti-Corruption **Policy**, and this Statement, as well as all applicable laws, rules, and regulations to which we are subject.

Q5: How does Digital Edge assess and manage modern slavery risks?

A: Understanding our modern slavery risk is critical to targeting our actions and partnerships to prevent and address the issue. Although **Digital Edge** does not operate in an industry sector with a high risk of

human trafficking and modern slavery, we acknowledge there are risks with regard to our indirect supply chain as well as certain geographic locations in which we operate. The risk is particularly high when any unskilled, temporary, or outsourced labor is involved. **Digital Edge** has adopted a Risk Management **Policy** that helps assess, monitor, and mitigate these risks.

Q6: What key performance indicators does Digital Edge use to monitor modern slavery risks?

A: We regularly assess our supply chain to determine whether any element may be of higher risk than previously assessed and/or requires us to undertake a physical audit. This is a continuous process. We are committed to physical inspections when our risk assessment determines it to be sensible. Our evaluation starts when a supplier is on-boarded and helps identify any high-risk suppliers. Suppliers are then subject to an on-going assessment process against a range of criteria, including compliance with our ethical standards and corporate values. Key suppliers are reviewed more frequently by the Legal Department and, if required, external advisors. We may also determine to conduct reviews and investigations on an ad-hoc basis, particularly if issues are raised by whistleblowers or on our ethics and compliance hotline.

Q7: What training does Digital Edge provide on modern slavery and trafficking?

A: **Digital Edge** has published our Code of Conduct and Business Partner Code of Conduct which set forth our expectations of ethical conduct from everyone performing services for or on behalf of **Digital Edge**. These codes are publicly available on **Digital Edge**'s website, and adherence to these Codes is a pre-condition to continued association with **Digital Edge**. Consistent with these codes, we expect all employees and Third Parties who work for us or on our behalf to ensure that human trafficking and modern slavery are never a part of **Digital Edge**'s supply chain or workplace. **Digital Edge** employees and business partners undergo periodic training to ensure compliance with these codes. Annual trainings are provided live and online and are available in multiple languages. Employees are required to certify compliance with and recommit to the Code on an annual basis.

Q8: How can I report concerns about human trafficking or modern slavery?

A: In addition to the training and codes, **Digital Edge** has adopted a Whistleblower **Policy** and maintains a helpline to address questions or concerns related to such Codes. **Digital Edge** enforces a zero tolerance, non-retaliation **Policy** that protects our employees when they raise a concern thereunder. You can raise concerns about suspected human trafficking or modern slavery without fear of retaliation. If you have questions about this Statement, or any situation or concern, contact Compliance Department vishal.jain@Digitaledgedc.com / Chief Legal & Compliance Officer joe.b@Digitaledgedc.com

Q9: What is Digital Edge's organizational structure and where does Digital Edge operate?

A: Headquartered in Singapore, **Digital Edge** is a trusted and forward-looking data center platform Company, established to transform digital infrastructure in Asia. Through building and operating state-of-the-art, energy-efficient data centers rich with connectivity options, **Digital Edge** aims to bring new colocation and interconnect options to the Asian market, making infrastructure deployment in the region easy, efficient, and economical. **Digital Edge** has operations in Singapore, Hong Kong, China, Korea, Japan, India, Indonesia, and the Philippines with a total of 15 data centers across eight metros.

Digital Edge is in the process of advancing plans for further metro and geographic expansion in the Asia Pacific region.

Q10: What does Digital Edge's supply chain look like and where are modern slavery risks?

A: **Digital Edge** provides space, power, HVAC, and related data center (including connectivity) services to our customers. In order to do so, **Digital Edge** must design and construct data centers, outfit the space with appropriate equipment and utilities, and provide appropriate functional support and oversight. Thus, **Digital Edge**'s supply chain contains a variety of suppliers, ranging from local to global. While **Digital Edge**'s equipment and infrastructure are often manufactured, supplied, and maintained by global suppliers and providers, **Digital Edge** also uses local support as needed for construction, security, maintenance, operation, and functional support. Although **Digital Edge** does not operate in an industry sector with a high risk of human trafficking and modern slavery, we acknowledge there are risks with regard to our indirect supply chain as well as certain geographic locations in which we operate. The risk is particularly high when any unskilled, temporary, or outsourced labor is involved.

TOOLS TO AVOID HUMAN TRAFFICKING AND MODERN SLAVERY

Digital Edge uses all available tools to avoid human trafficking and modern slavery:

- **Governance Programs: Digital Edge**-wide programs establishing oversight and accountability for compliance with anti-human trafficking and anti-modern slavery standards
- **Code of Conduct:** Sets forth expectations of ethical conduct from employees. Publicly available on **Digital Edge**'s website. Adherence is pre-condition to continued association with **Digital Edge**
- **Business Partner Code of Conduct:** Sets forth expectations of ethical conduct from third-party business partners. Publicly available on **Digital Edge**'s website. Adherence is pre-condition to continued association with **Digital Edge**
- **Third Party Due Diligence Policy and Procedures:** Establishes risk-based due diligence on all third parties with whom **Digital Edge** interacts. Promotes compliance with **Digital Edge Policies** and applicable laws
- **Whistleblower Policy:** Establishes helpline to address questions or concerns. Enforces zero tolerance, non-retaliation **Policy** protecting employees when they raise concerns
- **Contracting Terms and Conditions:** Contractual provisions requiring third parties to comply with anti-human trafficking and anti-modern slavery standards
- **Training Programs:** Periodic training for employees and business partners to ensure compliance with Codes. Annual training is provided live and online in multiple languages. Employees required to certify compliance with and recommit to Code on annual basis

---

RISK ASSESSMENT AND MANAGEMENT

Understanding modern slavery risk is critical to targeting actions and partnerships:

- **Industry Assessment: Digital Edge** does not operate in industry sector with high risk of human trafficking and modern slavery
- **Indirect Supply Chain Risks: Digital Edge** acknowledges risks with regard to indirect supply chain
- **Geographic Risks:** Risks acknowledged in certain geographic locations in which **Digital Edge** operates
- **Labor Type Risks:** Risk is particularly high when any unskilled, temporary, or outsourced labor is involved
- **Risk Management Policy: Digital Edge** has adopted **Policy** that helps assess, monitor, and mitigate modern slavery risks
- **Origin Assessment: Digital Edge** assesses potential human rights risks of supply chains by considering origin of suppliers
- **On-boarding Monitoring: Digital Edge** understands and monitors suppliers' approach to modern slavery as part of supplier on-boarding process
- **Direct Supplier Engagement: Digital Edge** actively engages with direct suppliers and thoroughly scrutinizes their management systems as it relates to their upstream suppliers

---

KEY PERFORMANCE INDICATORS

Digital Edge regularly assesses supply chain through continuous process:

- **Regular Supply Chain Assessment: Digital Edge** regularly assesses supply chain to determine whether any element may be of higher risk than previously assessed and/or requires physical audit
- **Physical Inspections: Digital Edge** is committed to physical inspections when risk assessment determines it to be sensible
- **Supplier On-boarding Evaluation:** Evaluation starts when supplier is on-boarded and helps identify any high-risk suppliers
- **On-going Assessment Process:** Suppliers subject to on-going assessment process against range of criteria, including compliance with ethical standards and corporate values
- **Key Supplier Reviews:** Key suppliers reviewed more frequently by Legal Department and, if required, external advisors
- **Ad-hoc Reviews and Investigations: Digital Edge** may determine to conduct reviews and investigations on ad-hoc basis, particularly if issues raised by whistleblowers or on ethics and compliance hotline

---

TRAINING REQUIREMENTS

All employees and business partners must undergo training:

- **Code Publication: Digital Edge** has published Code of Conduct and Business Partner Code of Conduct which set forth expectations of ethical conduct from everyone performing services for or on behalf of **Digital Edge**
- **Public Availability:** Codes are publicly available on **Digital Edge**'s website
- **Pre-condition to Association:** Adherence to Codes is pre-condition to continued association with **Digital Edge**
- **Supply Chain and Workplace Expectation:** All employees and Third Parties who work for **Digital Edge** or on **Digital Edge**'s behalf must ensure that human trafficking and modern slavery are never a part of **Digital Edge**'s supply chain or workplace
- **Periodic Training: Digital Edge** employees and business partners undergo periodic training to ensure compliance with Codes
- **Annual Trainings:** Annual trainings are provided live and online and are available in multiple languages
- **Annual Certification:** Employees are required to certify compliance with and recommit to Code on annual basis

---

REPORTING MECHANISMS

Multiple channels available for reporting concerns:

- **Whistleblower Policy and Helpline: Digital Edge** has adopted Whistleblower **Policy** and maintains helpline to address questions or concerns related to Codes
- **Zero Tolerance, Non-Retaliation Policy: Digital Edge** enforces zero tolerance, non-retaliation **Policy** that protects employees when they raise concerns
- **Ethics and Compliance Hotline:** Available for reporting issues that may trigger ad-hoc reviews and investigations
- **Policy Representative:** Contact Compliance Department if you have questions about this Statement, or any situation or concern

---

REMEMBER

Human trafficking and modern slavery are violations of fundamental human rights and are intended to exploit vulnerable persons for the gratification or commercial gain of others. Digital Edge is committed to ensuring that human trafficking and modern slavery never play a part in our workplace or in our supply chain. Digital Edge has a zero-tolerance Policy for any instances of human trafficking or modern slavery, and we demand the same opposition from all who work for or with us. All employees and third-party business partners must comply with the Code of Conduct and Business Partner Code of Conduct, which are publicly available on Digital Edge's website. Adherence to these Codes is a pre-condition to continued association with Digital Edge. You must undergo periodic training and certify compliance with the Code on an annual basis. If you have questions or concerns about human trafficking or modern slavery, use the Whistleblower Policy and helpline without fear of retaliation. Digital Edge enforces a zero tolerance, non-retaliation Policy that protects employees when they raise concerns. Contact Policy Representative Compliance Department vishal.jain@digitaledgedc.com if you have questions about this Statement or any situation or concern.

DATA PRIVACY AND ACCESS GUIDELINES

This section provides a high-level overview of Digital Edge's Data Privacy and Access Guidelines for ease of reference. Employees should refer to the detailed Data Privacy and Access Guidelines Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

Digital Edge collect, maintain, and process a wide variety of data during the course of their operations. Some of this data will invariably include Personal Data collected directly from Data Subjects—these Data Subjects can range from employees, customers, prospective customers, and/or suppliers. Regulators around the world have or are beginning to issue guidelines on how to handle this Personal Data, known as Data Privacy Laws. Failure to adhere to these privacy laws can bring severe consequences to **Digital Edge**, often in the form of astronomical fines.

Key Principles:

- **Digital Edge** is committed to complying with Data Privacy Laws and protecting privacy and security of Personal Data
- Personal Data includes any information that personally identifies or may be used to personally identify a Data Subject
- Sensitive Personal Data includes health information, racial/ethnic origin, political/religious views, biometric information, financial information
- **Digital Edge** collects Personal Data from customers, business partners, suppliers, and Personnel for legitimate business activities
- Personal Data only collected and used for legitimate business activities and as required/permitted by law
- **Digital Edge** transfers, processes, and stores Personal Data in accordance with Data Protection Laws
- **Digital Edge** retains Personal Data only as long as necessary to fulfill collection purpose
- Data Subjects notified about collection, use, transfer, and disclosure of their Personal Data
- Personnel may access Personal Data only if authorized as part of their job and only for authorized purpose
- Personnel must be vigilant in safeguarding Personal Data and report breaches immediately
- Data Subjects have rights to access, correct, erase, or block Personal Data held about them
- Personal Data breaches must be reported immediately in accordance with Security Incident Management **Policy**
- Violation of **Policy** may result in disciplinary measures up to and including termination
- Misuse of Personal Data may subject Personnel and **Digital Edge** to civil or criminal penalties

If you become aware of, or suspect, a Personal Data breach, you must report that breach immediately in accordance with the Cyber Security Incident Response Plan. You should not attempt to take any steps on your own without clearance from the Head of IT and/or Compliance Department.

POLICY OBJECTIVE

The purpose of this **Policy** is to inform Personnel of the standards that they need to adhere to if and when they handle Personal Data or if they are or become aware of any Personal Data not being handled in a proper manner. This **Policy** also seeks to explain the various initiatives that **Digital Edge** has undertaken and intends to undertake to ensure compliance with various Data Privacy Laws. The **Policy** is designed to:

- Describe measures taken to protect Personal Data
- Explain Data Subject rights regarding Personal Data collected about them
- Define Personnel responsibilities to protect Personal Data while at **Digital Edge**
- Provide guidance on what to do if receiving a request for Personal Data or suspecting/aware of data breach
- Establish standards for collection, processing, storing, transferring, archiving, and destruction of Personal Data
- Define **Digital Edge**'s commitment to complying with Data Privacy Laws globally
- Clarify lawful bases for processing Personal Data (contractual obligations, legal compliance, legitimate interests)
- Establish procedures for transferring Personal Data to other DE Entities and external third parties
- Define retention and destruction procedures for Personal Data
- Establish notification and consent requirements for Data Subjects
- Describe **Digital Edge**'s multi-faceted approach to ensuring data privacy compliance
- Define Data Subject rights (access, accuracy, correction, erasure, objection to processing)
- Establish incident response plan and breach notification process
- Require Personnel vigilance, authorized access only, proper handling of requests, and attendance at training
- Impose discipline on Personnel found to have violated this **Policy**

Training on privacy matters is offered to all employees. If you regularly receive, handle, or process Personal Data in your role with Digital Edge, you are encouraged to attend these trainings. Digital Edge may mandatorily require you to undertake this training depending on your role or position.

DOs AND DON'Ts

DOs

DO comply with this **Policy** and all Personnel obligations regarding Personal Data

DO understand that Data Privacy Laws protect Personal Data of individuals by imposing restrictions on collection, processing, storing, transferring, archiving, and destruction

DO be aware that **Digital Edge** collects Personal Data from customers, business partners, suppliers, and Personnel

DO know that Personal Data includes any information that personally identifies or may be used to personally identify a Data Subject

DO understand that Sensitive Personal Data includes health information, racial/ethnic origin, political/religious views, trade union membership, sexual orientation, biometric information, criminal offenses, and financial information

DO be aware that Processing means any operation performed on Personal Data including collection, recording, organization, storage, adaptation, retrieval, use, disclosure, transmission, erasure, or destruction

DO recognize that **Digital Edge** collects Personal Data from customers/prospective customers and business partners to fulfill contractual obligations, manage accounts, monitor compliance, market new products/services, and for business operations

DO understand **Digital Edge** collects Personnel Personal Data for recruitment, payroll, employee administration, compensation, promotion, performance review, learning management, expense reporting, benefits management, and data storage/processing

DO understand **Digital Edge** may transfer, process, and store Personal Data outside country of collection in accordance with Data Protection Laws

DO know each DE Entity has entered into Inter-Affiliate Data Transfer Agreement (DTA) specifying standards for collecting, storing, processing, and transferring Personal Data

DO be aware **Digital Edge** takes reasonable steps to ensure external third-party service providers comply with Data Protection Laws

DO know **Digital Edge** notifies Data Subjects about collection, use, transfer, and disclosure of their Personal Data and obtains consent where required

DO review **Digital Edge**'s Website Privacy **Policy** at https://www.digitaledgedc.com/privacy-**Policy**

DO review **Digital Edge**'s Cookie **Policy** at https://www.digitaledgedc.com/cookies-**Policies**

DO understand **Digital Edge** conducts data privacy reviews, risk assessments, and audits on as-needed basis

DO attend training on privacy, data protection, and information security as required by **Digital Edge**

DO ensure any proposed marketing campaign is in compliance with applicable Data Protection Laws

DO consult with Legal / Compliance Department regarding marketing activities in any country

DO refer to **Digital Edge**'s SharePoint for IT Security Team **Policies** on network security safeguards

DO understand you have rights as Data Subject to access, correct, erase, or block Personal Data held about you

DO contact appropriate Privacy Point of Contact if you want to exercise your Data Subject rights or have questions

DO contact Chief Legal and Compliance Office or Compliance Department for data privacy issues

DO read and familiarize yourself with Security Incident Management **Policy** and Procedures and Cyber Security Incident Response Plan

DO report suspected or actual Personal Data breach immediately in accordance with Cyber Security Incident Response Plan

DO render assistance as may be reasonably necessary if called upon to assist in investigation of Personal Data breach

DO be vigilant in safeguarding Personal Data of customers and other Personnel

DO access and use Personal Data only if you are authorized to do so as part of your job and only for purpose for which you are authorized

DO direct requests for Personal Data from persons other than Data Subject to Compliance Department

DO contact Compliance Team immediately if customer raises questions, complaints, or disputes regarding their Personal Data

DO contact Compliance Department if working on new product, service, or project that involves collection, processing, transfer, or storage of Personal Data or use of cloud by third party

DO attend training on privacy matters as required by Compliance Department

DO determine if information is Personal Data by considering if it allows you to identify an individual either directly or indirectly

DO keep Personal Data in paper form in locked filing cabinets or equivalent storage for safekeeping

DO shred printouts containing Personal Data before disposal

DO use Personal Data only for purpose for which it was collected

DO immediately report to Compliance Department if you think your Personal Data may have been disclosed to unauthorized parties without consent

DO contact appropriate Privacy Point of Contact if you have concerns about accuracy of your Personal Data

DO ensure external service providers process Personal Data in line with **Digital Edge**'s **Policies** and procedures

DO ensure Personal Data is only transferred to service provider if there is contract requiring appropriate security and processing only as per **Digital Edge**'s instructions

DO regularly audit Personal Data you hold and delete anything you no longer need

DO retain Personal Data only for so long as strictly necessary to fulfill purpose for which it was collected

DO understand obligations under **Policy** apply throughout period you hold or process Personal Data

DON'Ts

DON'T collect or use Personal Data for purposes other than legitimate business activities or as required/permitted by law

DON'T transfer Personal Data outside country of collection except where permitted by and within constraints of applicable Data Protection Laws

DON'T retain Personal Data for longer than necessary to fulfill purpose for which it is collected

DON'T fail to notify Data Subjects about collection, use, transfer, and disclosure of their Personal Data where required

DON'T fail to obtain consent from Data Subjects where required by applicable Data Protection Laws

DON'T neglect to review and comply with **Digital Edge**'s Website Privacy **Policy** and Cookie **Policy**

DON'T engage in marketing activities without ensuring compliance with applicable Data Protection Laws

DON'T fail to consult with Compliance Department regarding marketing activities in any country

DON'T deny Data Subjects their rights to access, correct, erase, or block Personal Data held about them

DON'T delay in responding to Data Subject requests (**Digital Edge** has very short period of time to respond)

DON'T attempt to take any steps on your own without clearance from Head of IT and/or Compliance Department when Personal Data breach occurs

DON'T fail to assist in investigation of Personal Data breach when called upon

DON'T access or use Personal Data if you are not authorized to do so as part of your job

DON'T use Personal Data for purposes other than those for which you are authorized

DON'T respond to requests for Personal Data from persons other than Data Subject without directing them to Compliance Department

DON'T delay contacting Compliance Team when customer raises questions, complaints, or disputes regarding their Personal Data

DON'T work on new products, services, or projects involving Personal Data without contacting Compliance Department

DON'T refuse to attend training on privacy matters as required by Compliance Department (failure may result in disciplinary action)

DON'T leave records containing Personal Data unattended on your desk

DON'T use Personal Data for purposes other than those for which it was collected

DON'T fail to report incidents where your Personal Data may have been disclosed to unauthorized parties

DON'T neglect to address concerns about accuracy of your Personal Data

DON'T engage external service providers to process Personal Data without ensuring they comply with **Digital Edge**'s **Policies** and procedures

DON'T transfer Personal Data to service providers without contract requiring appropriate security and processing per **Digital Edge**'s instructions

DON'T fail to regularly audit Personal Data you hold or delete data you no longer need

DON'T retain Personal Data beyond period strictly necessary to fulfill purpose for which it was collected

DON'T fail to comply with **Policy** from moment you obtain Personal Data until time when Personal Data has been returned, deleted, or destroyed

---

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What is Personal Data and how do I determine what is or is not Personal Data?

A: Personal Data is any information that identifies or could be used to identify a Data Subject, either directly or in combination with other data. The simple test for identifying Personal Data is whether the information such as an employee ID, passport number, phone number, or email address which allows you to distinguish a specific individual. This data can exist in any form, including paper records, IT systems, or CCTV images. Other examples include an individual's date of birth, address, passport number, or credit card details. Business cards, phone numbers, and email addresses exchanged during calls or business meetings are considered Personal Data because they allow you to identify an individual. If you are uncertain whether any information is considered Personal Data, contact the Compliance Department for clarification.

Q2: What is Sensitive Personal Data and how is it different from Personal Data?

A: Sensitive Personal Data means Personal Data relating to physical or mental health, racial or ethnic origin, political or religious views, trade union membership, sexual orientation, medical or health information, biometric information, and the commission or alleged commission of offenses and related proceedings, and, in some countries, financial information, or as that term is otherwise defined under applicable Data Protection Law. Sensitive Personal Data is a subset of Personal Data that requires heightened protection due to its sensitive nature. All Sensitive Personal Data is Personal Data, but not all Personal Data is Sensitive Personal Data. For purposes of this **Policy**, the term Personal Data also includes Sensitive Personal Data unless necessary to distinguish between the terms.

Q3: What does "handling" or "processing" Personal Data mean and what kinds of activities in my daily job would involve this?

A: Processing means any operation or set of operations that is performed on Personal Data, whether by automatic means or otherwise, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. Handling Personal Data is also known as processing Personal Data. This covers practically anything that can be done with information—obtaining it, viewing it, collecting it, sorting it, analyzing it, discussing it, destroying it, or even just filing it.

Q4: How does Digital Edge collect Personal Data and for what purposes?

A: **Digital Edge** collects Personal Data from two primary sources: external business partners and their own personnel. Data from customers and suppliers is collected to manage accounts, fulfill contracts, and perform business operations like billing and marketing. Personnel data is collected for employment-related purposes, including payroll, recruitment, benefits management, and performance reviews. The scope of Personal Data collected may vary based on certain factors such as local requirements. **Digital Edge** only collects and uses Personal Data for legitimate business activities and as may be required and/or permitted by law.

Q5: How does Digital Edge transfer and store Personal Data?

A: In addition to collecting Personal Data, **Digital Edge** may transfer, process, and store Personal Data outside of the country in which it collected such Personal Data. This may include a transfer to another DE Entity other than the DE Entity that collected the Personal Data or to an external third party. **Digital Edge** will only transfer any Personal Data where permitted by, and within the constraints of, applicable Data Protection Laws and applicable data security commitments. For purposes of Data Protection Laws, transfers to another DE Entity are considered transfers to third parties. Each DE Entity has entered into an Inter-Affiliate Data Transfer Agreement (DTA) which specifies the standards to be met by each DE Entity when it collects, stores, processes, and transfers Personal Data to ensure all DE Entities meet a recognized standard. Where **Digital Edge** engages an external third-party service provider/vendor to perform activities that may require access to Personal Data, **Digital Edge** will take reasonable steps to ensure applicable Data Protection Laws are complied with, such as requiring the service provider/vendor to act in accordance with **Digital Edge**'s existing **Policies** and procedures and all applicable Data Protection Laws.

Q6: What are my rights as a Data Subject regarding Personal Data Digital Edge holds about me?

A: You have certain rights as a Data Subject, and these are conferred under applicable Data Protection Laws. **Digital Edge** respects the privacy of its Personnel and accords all Personnel the following rights: (1) To access certain Personal Data held about the Personnel in question; (2) To ensure that any Personal Data held is accurate and relevant to the purposes for which **Digital Edge** collected the Personal Data; (3) To correct, erase, or block any Personal Data that is incorrect about the Personnel in question; and (4) To object to the processing of his or her Personal Data based on compelling, legitimate grounds relating to his or her particular situation, to the extent permitted under applicable Data Protection Laws in the country in which the Personal Data was collected. If you want to exercise any of your rights as a Data Subject or have any questions about your rights regarding Personal Data **Digital Edge** collects about you, you should contact the appropriate point of contact: Chief Legal and Compliance Officer: joe.b@digitaledgedc.com or Compliance Department: vishal.jain@digitaledgedc.com **Digital Edge** will comply with the rights of Data Subjects based on the Data Protection Laws of their particular jurisdiction, including any laws relating to editing, correcting, updating, and providing access to Personal Data.

Q7: What is a Personal Data breach and what should I do if I suspect or become aware of one?

A: A Personal Data breach has occurred when Personal Data, whether intentionally or unintentionally, is, or is put at risk of being, disclosed to any person or entity that is not authorized to have access to that Personal Data. Examples of Personal Data breaches could involve the loss of a device or document (e.g., laptop, wireless phone containing unencrypted Personal Data), theft of devices, computer incidents (e.g., denial of service/distributed denial of service attacks, firewall breaches), and accidental disclosure. You are required to report a suspected or actual Personal Data breach immediately—it is very important that you do so. Note that in some countries, **Digital Edge** is obliged to report data breaches in a very short amount of time, and it is therefore important that you follow the process immediately upon becoming aware of or suspecting a breach. You should not attempt to take any steps on your own without clearance from the Head of IT and/or Compliance Department.

Q8: What do I need to do to safeguard the Personal Data in my possession?

A: As stated in the **Policy**, you may access and use Personal Data only if you are authorized to do so as part of your job or function. You must always be vigilant while handling Personal Data. If the Personal Data is in paper form, it should be kept in locked filing cabinets or equivalent storage for safekeeping. Never leave records containing Personal Data unattended on your desk. Printouts containing Personal Data must be shredded before disposal. For more details, refer to the suite of Corporate Security **Policies** on the intranet. Remember that all Personal Data must only be used for the purpose for which it was collected and if you are handling Personal Data, then the responsibility for handling it properly rests with you. The basic principle to follow is that you must retain Personal Data only for so long as it is strictly necessary to fulfill the purpose for which it was collected. It is best that you regularly audit the Personal Data you hold and delete anything you no longer need.

Q9: What should I do if I receive a request for Personal Data or if a customer raises questions about their Personal Data?

A: **Digital Edge** may receive requests for Personal Data from law enforcement or persons other than the Data Subject. If you receive a request for Personal Data from any person other than the Data Subject, please direct that request to the Compliance Department. If a customer raises any questions, complaints, or disputes regarding the collection, use, and disclosure of their Personal Data, you must contact the Compliance Team immediately. **Digital Edge** has a very short period of time in which to respond to the customer's request, so prompt action is critical. **Digital Edge** will promptly investigate and attempt to resolve customer, vendor, and other third-party complaints and disputes in a manner that complies with the principles described in this **Policy**, applicable Data Protection Laws, and the terms of the relevant contract.

Q10: What should I do if I'm working on a new product, service, or project that involves Personal Data or engaging an external service provider?

A: If you are working on a new product, service, project, etc., for **Digital Edge** that involves (a) the collection, processing, transfer and/or storage of any Personal Data, and/or (b) the use of a cloud by a third party for the storage of any Personal Data, you are required to contact the Compliance Department so that they can assess the impact of any relevant Data Protection Laws and advise you accordingly on how you may proceed. Regarding external service providers: Please remember that you are directly responsible for making sure that the external service provider engaged by you processes the Personal Data in line with **Digital Edge**'s **Policies** and procedures. In particular, you should ensure that Personal Data is only transferred to a service provider if there is a contract requiring the service provider to maintain appropriate security for all Personal Data shared and process such Personal Data only as per **Digital Edge**'s instructions. If you are unsure as to any of the above, you should contact the Compliance Department for assistance.

DATA SUBJECT RIGHTS SUMMARY

All Personnel and third parties from whom Digital Edge collects Personal Data have the following rights:

- **Right to Access:** To access certain Personal Data held about the Personnel or third party in question
- **Right to Accuracy:** To ensure that any Personal Data held is accurate and relevant to the purposes for which **Digital Edge** collected the Personal Data
- **Right to Correction/Erasure:** To correct, erase, or block any Personal Data that is incorrect about the Personnel or third party in question
- **Right to Object:** To object to the processing of his or her Personal Data based on compelling, legitimate grounds relating to his or her particular situation, to the extent permitted under applicable Data Protection Laws in the country in which the Personal Data was collected

To exercise Data Subject rights or report complaints:

- Contact Chief Legal and Compliance Office: joe.b@digitaledgedc.com
- Contact Compliance Department: vishal.jain@digitaledgedc.com

Digital Edge will comply with rights of Data Subjects based on Data Protection Laws of their applicable jurisdiction.

PERSONNEL COMPLIANCE OBLIGATIONS

All Personnel must adhere to the following compliance steps:

- **Vigilance:** Personnel have obligation to be vigilant in safeguarding Personal Data of customers and other Personnel. If you become aware of, or suspect, a Personal Data breach, you must report that breach immediately in accordance with Cyber Security Incident Response Plan.
- **Authorized Access Only:** You may access and use Personal Data only if you are authorized to do so as part of your job, and only for the purpose for which you are authorized.
- **Requests for Personal Data: Digital Edge** may receive requests for Personal Data from law enforcement or persons other than Data Subject. If you receive request for Personal Data from any person other than Data Subject, direct that request to Compliance l Department.
- **Customer Inquiries:** If customer raises any questions, complaints, or disputes regarding collection, use, and disclosure of their Personal Data, contact Compliance Compliance Team immediately.
- **New Products/Services/Projects:** If working on new product, service, project, etc., for **Digital Edge** that involves (a) collection, processing, transfer and/or storage of any Personal Data, and/or (b) use of cloud by third party for storage of any Personal Data, contact Compliance Department for assessment and advice.

- **Training Attendance:** As Data Protection Laws are constantly evolving, Compliance Department may require you to attend training on privacy matters from time to time. You are required to attend any such training and failure to do so may result in disciplinary action.
- **Safeguarding Personal Data:** Keep Personal Data in paper form in locked filing cabinets or equivalent storage. Never leave records containing Personal Data unattended on your desk. Shred printouts containing Personal Data before disposal.
- **Purpose Limitation:** Use Personal Data only for purpose for which it was collected.
- **Regular Audits:** Regularly audit Personal Data you hold and delete anything you no longer need.
- **Retention Limitation:** Retain Personal Data only for so long as strictly necessary to fulfill purpose for which it was collected.

Violation of any provision of this Policy may subject Personnel to disciplinary measures up to and including termination of employment and/or engagement by Digital Edge. Misuse of Personal Data also may subject you and Digital Edge to civil or criminal penalties by applicable Data Protection Authority or other government entities.

DIGITAL EDGE INITIATIVES FOR DATA PRIVACY COMPLIANCE

Digital Edge has implemented a multi-faceted approach to ensure compliance with Data Protection Laws:

- **Review of Information Collection Practices: Digital Edge** has reviewed its information collection procedures, including interviewing certain Personnel about data collection practices. **Digital Edge** will re-evaluate data collection practices as needed and may update **Policy** from time to time.
- **Data Privacy Policies: Digital Edge** has made publicly available data privacy-related **Policies** including Website Privacy **Policy** (https://www.digitaledgedc.com/privacy-**Policy**) and Cookie **Policy** (https://www.digitaledgedc.com/cookies-**Policies**).
- **Inter-Affiliate Data Transfer Agreement:** Each DE Entity has signed DTA which addresses procedures that applicable DE Entity is to take before it transfers Personal Data outside of country of collection.
- **Continued Risk Assessment and Audit: Digital Edge** conducts data privacy reviews on as-needed basis and reviews/identifies whether any new Personnel, customer, product, or creation of new database triggers any new data privacy risk. **Digital Edge** conducts periodic audits to review **Digital Edge**'s and Personnel's compliance with this and other data privacy-related **Policies**.
- **Training: Digital Edge** trains Personnel regarding privacy, data protection, and information security including overview of Personal Data maintained, purposes for maintaining Personal Data, responsibility to protect Personal Data, and obligations **Digital Edge** has taken.
- **Marketing Compliance:** Marketing Team is responsible for ensuring any proposed marketing campaign is in compliance with applicable Data Protection Laws. All

Personnel must adhere to **Policies** and procedures released by Marketing Team regarding conduct of any marketing activities or campaigns.

- **Network Security/Safeguards: Digital Edge** has implemented appropriate technical and organizational security measures to protect against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other forms of unlawful processing. Refer to **Digital Edge**'s SharePoint for IT Security Team **Policies**.
- **Ensuring Integrity of Personal Data: Digital Edge** is committed to ensuring Personal Data collected is (1) accurate and, where necessary, kept up to date; (2) adequate, relevant, and not excessive in relation to purposes for which it is collected or may be transferred; and (3) not processed and/or retained for longer than necessary for purposes for which it is collected.

INCIDENT RESPONSE AND BREACH NOTIFICATION

Digital Edge's IT Security Team has established incident response plan in its Security Incident Management Policy and Procedures.

How to Access Incident Response Plan:

- Click on Cyber Security Incident Response Plan link on **Digital Edge** SharePoint
- You are encouraged to read Security Incident Management **Policy** and Procedures and ensure you are familiar with process

Examples of Personal Data Breaches:

- Loss of device or document containing unencrypted Personal Data (laptop, wireless phone, etc.)
- Theft of devices
- Computer incidents (denial of service/distributed denial of service attacks, firewall breaches, etc.)
- Accidental disclosure (e.g., sending email containing customer's bank details to wrong recipient)

Critical Requirements:

- Report suspected or actual Personal Data breach immediately
- It is very important that you report immediately
- Do not attempt to take any steps on your own without clearance from Head of IT and/or Compliance Department
- In some countries, **Digital Edge** is obliged to report data breaches in very short amount of time
- Follow process immediately upon becoming aware of or suspecting breach

Investigation Process:

- Any investigation will be conducted pursuant to Security Incident Management **Policy** and Procedures
- If called upon to assist in investigation of Personal Data breach, you are required to render such assistance as may be reasonably necessary

---

CONSEQUENCES OF NON-COMPLIANCE

Disciplinary Measures:

Violation of any provision of this **Policy** may subject Personnel to disciplinary measures up to and including termination of employment and/or engagement by **Digital Edge**

Legal Penalties:

- Misuse of Personal Data also may subject you and **Digital Edge** to civil or criminal penalties by applicable Data Protection Authority or other government entity
- Failure to adhere to Data Privacy Laws can bring severe consequences to **Digital Edge**, often in form of astronomical fines

Data Subject Complaint Process:

- **Digital Edge** will, in good faith, work to remedy any breach of Data Subject's rights under this **Policy**
- With regard to Personnel: If you have any complaint, or if you dispute collection, use, and disclosure of your Personal Data, contact appropriate Privacy Point of Contact
- With regard to customers, vendors, and third parties: **Digital Edge** will promptly investigate and attempt to resolve complaints and disputes in manner that complies with principles described in **Policy**, applicable Data Protection Laws, and terms of relevant contract

---

CONTACTS FOR GUIDANCE

Compliance Department

For questions about this **Policy** and data privacy generally. About Data Protection Laws, requests for Personal Data, customer inquiries, new products/services/projects involving Personal Data, external service provider contracts, and data privacy compliance. Contact immediately if customer raises questions, complaints, or disputes regarding their Personal Data.

Head of IT

For clearance before taking any steps when Personal Data breach occurs.

Marketing Team

For guidance on ensuring marketing campaigns comply with applicable Data Protection Laws.

IT Security Team

Refer to **Digital Edge**'s SharePoint for IT Security Team **Policies** on network security safeguards.

POLICY UPDATES AND RESOURCES

Policy Amendments:

- This **Policy** may be amended from time to time, as required and/or permitted by applicable Data Protection Laws
- Copy of current version of **Policy** will be posted on Legal Department's **Policies** and Procedures page of **Digital Edge**'s SharePoint page

Additional Resources:

- Website Privacy **Policy**: https://www.digitaledgedc.com/privacy-**Policy**
- Cookie **Policy**: https://www.digitaledgedc.com/cookies-**Policies**
- Security Incident Management **Policy** and Procedures (**Digital Edge** SharePoint)
- Cyber Security Incident Response Plan (**Digital Edge** SharePoint)
- Corporate Security **Policies** (**Digital Edge** Intranet)
- IT Security Team **Policies** (**Digital Edge** SharePoint)
- Records Management **Policy** (referenced for destruction of Personal Data)

Training:

- **Digital Edge** offers training on privacy matters generally to all employees
- If you regularly receive, handle, or process Personal Data in your role, you are encouraged to attend these trainings
- **Digital Edge** may mandatorily require you to undertake this training depending on your role or position within **Digital Edge**
- Legal / Compliance Department may require you to attend training on privacy matters from time to time as Data Protection Laws constantly evolve

---

REMEMBER

Digital Edge is committed to complying with Data Privacy Laws and protecting the privacy and security of Personal Data in our possession. You may access and use Personal Data only if you are authorized to do so as part of your job, and only for the purpose for which you are authorized. You must be vigilant in safeguarding Personal Data of customers and other Personnel. If you become aware of, or suspect, a Personal Data breach, you must report that breach immediately in accordance with the Cyber Security Incident Response Plan. Do not attempt to take any steps on your own without clearance from the Head of IT and/or Compliance Department. Never leave records containing Personal Data unattended on your desk. Shred printouts containing Personal Data before disposal. Use Personal Data only for the purpose for which it was collected. Regularly audit the Personal Data you hold and delete anything you no longer need. Your obligations under this Policy apply throughout the period that you hold or process Personal Data—from the moment you obtain the Personal Data until the time when the Personal Data has been returned, deleted, or destroyed. Violation of this Policy may result in disciplinary measures up to and including termination of employment and may subject you and Digital Edge to civil or criminal penalties.

BUSINESS TRAVEL AND EXPENSE REIMBURSEMENT POLICY

This section provides a high-level overview of Digital Edge's Business Travel and Expense Reimbursement Policy for ease of reference. Employees should refer to the detailed Business Travel and Expense Reimbursement Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

The Business Travel and Expense Reimbursement **Policy** ("**Policy**") provide standards and procedures for incurring and seeking reimbursement of authorized expenses. **Digital Edge** is committed to providing clear guidance on what expenses are authorized and uniform rules for their timely reimbursement.

You may incur and will be reimbursed for expenses that are authorized in this **Policy**. If an expense is not authorized, you are prohibited from incurring it and, if incurred and reimbursed by **Digital Edge**, you may be required to repay it and any reimbursement may be classified as taxable compensation to you. In addition, failure to comply with this **Policy** may result in disciplinary action.

Key Principles:

- Only expenses authorized in this **Policy** are reimbursable
- Unauthorized expenses may result in repayment and/or classification as taxable compensation
- Managers and employees share responsibility for ensuring compliance
- International travel requires prior written approval from direct supervisor and Director Level executive to which the said employee reports.
- Domestic air travel requires pre-approval from direct supervisor or manager
- Airline class of service determined by employee grade and flight duration
- First Class travel is never permitted
- Accommodation limited to standard single rooms at reasonably priced hotels
- Personal meals and business entertainment have specific requirements
- All expense reports must use **Digital Edge**'s web-based automated expense reporting application
- Expense reports should be submitted within 30 business days after completion of trip
- Non-compliance may result in disciplinary action up to and including dismissal
- Violations must be reported to Country Finance Head (in the first instance) or Ethics Hotline
- Periodic audits and investigations will be conducted

POLICY OBJECTIVE

The purpose of this **Policy** is to establish clear standards and procedures for incurring and seeking reimbursement of authorized business travel, entertainment, and other expenses.

This Policy is designed to:

- Provide clear guidance on what expenses are authorized for reimbursement
- Establish uniform rules for timely reimbursement of authorized expenses
- Define manager and employee responsibilities for compliance
- Clarify travel approval requirements (international and domestic)
- Establish airline class of service standards based on employee grade and flight duration
- Define accommodation standards and reimbursable lodging expenses
- Clarify automobile rental and personal vehicle reimbursement procedures
- Establish personal meal and business entertainment reimbursement criteria
- Define non-reimbursable expenses and prohibited expenditures
- Establish expense reporting, approval, and payment procedures
- Implement controls to ensure compliance with **Policy** requirements
- Prevent and detect violations through periodic audits and investigations
- Impose discipline on individuals found to have breached this **Policy**
- Protect both **Digital Edge** and employees regarding tax implications

Expense reports are meant for reimbursement or payment of business travel, entertainment, and other expenses as outlined in this Policy. The purchasing of business goods and services is covered under a separate set of Policies and procedures.

DOs AND DON'Ts

DOs

DO comply with the **Policies** and procedures outlined in this **Policy**

DO control the cost of travel as is reasonable under the circumstances

DO ensure submission of accurate expense reports

DO identify and pay for personal expenses

DO obtain prior written approval from direct supervisor and Director Level executive for all international travel

DO obtain pre-approval from direct supervisor or manager for domestic air travel

DO submit Pre-Travel Authorization Form (Annexure I) for all travel approval requests

DO attempt to book tickets in the least costly manner

DO use online booking sites where possible for routine non-complex travel

DO schedule airline reservations 14 days in advance but not less than 5 days prior to travel

DO attach original passenger receipt to Expense Report for reimbursement

DO book non-refundable airfare tickets where possible as cost is significantly less expensive

DO use most direct route between origination and destination points when calculating flight-time

DO select most cost-effective airport parking options (utilize Long-Term parking when available)

DO attempt to secure complimentary accommodation from airline if delay requires overnight stay

DO return unused or partially used airline tickets to booking agent/airline for reimbursement as soon as possible

DO contact booking agent or airline about using same ticket for future travel when trip is cancelled

DO book accommodation at hotels with **Digital Edge** corporate rates or use web booking sites

DO accept room upgrades to suites or executive floor rooms if at no additional cost to **Digital Edge**

DO contact hotel directly to seek long-term stay discounts if staying a week or longer

DO inquire about long-term stay discounts or service apartments for ongoing projects (1 month+)

DO cancel hotel reservations within hotel's cancellation **Policy** time frame

DO keep cancellation number until credit card statement verifies no charges applied

DO inspect rental vehicle for any damage prior to leaving car rental lot

DO return rental cars with full tank of fuel to minimize refueling surcharges

DO attach refueling receipts to expense report

DO take Liability and Collision insurance offered by rental **Digital Edge**

DO have sufficient automobile liability and property damage insurance coverage when using personal vehicle

DO submit clear description of business purpose, start/end points, and number of miles/kilometers for personal vehicle reimbursement

DO check with Finance Department to ascertain current mileage reimbursement amount in your location

DO utilize most economical and safest mode of transportation available

DO consider use of local transportation (hotel shuttles, taxis, public transportation)

DO properly identify individual transportation expenditures on expense report

DO dine at reasonably priced establishments while on business travel

DO provide explanation for expense if receipts are not available

DO attach itemized original receipts for all expenses

DO limit gratuities and tips to accepted norm within country

DO use internet calling (WhatsApp, Line) when available rather than mobile service or hotel room calls

DO know and understand all immunization, inoculation, passport, and visa requirements prior to international travel

DO maintain current passport with suitable remaining valid term where you expect to travel

DO ensure primary purpose of trip is business if including personal travel

DO ensure no extra expense to **Digital Edge** and personal travel does not interfere with business objective

DO ensure business meals and entertainment comply with Gift & Entertainment **Policy**

DO ensure entertainment is directly related to active conduct of business

DO ensure entertainment is directly preceded or followed by substantial and bona fide business discussion

DO provide full list of attendees, titles, Company names, and reason for expenditure when submitting claim

DO attach receipts for ALL entertainment expenses

DO ensure most senior person attending function makes payment for entire event

DO discuss and agree pro-rata approach with Finance Department for bundled or family phone plans

DO apply to Country Manager for contribution to home internet plan and home office expenses

DO ensure gifts are **Digital Edge**-logoed items or of nominal value only

DO list gift recipient's name, Company, and position with submission of expense report

DO use Purchase Requisition or Payment Request Form for operating goods or capital equipment

DO obtain written pre-approval from Finance if miscellaneous expenditure exceeds US$1,500

DO use **Digital Edge**'s web-based automated expense reporting application to submit expenses

DO include all required information in expense report (employee name/code, dates, cost center, purpose, cities, itemized costs, VAT/GST disclosure, receipts, Pre-Trip Authorization Form, signatures)

DO ensure prompt and accurate submission of Expense Reports within 30 business days after completion of trip

DO review expense report for accuracy before submitting to manager for approval

DO contact country finance team for assistance updating bank account

DO promptly report witnessed behavior that may represent a violation of this **Policy**

DO raise concerns with manager or Finance Department if expenditure on own account presents cashflow issue

DON'Ts

DON'T incur expenses that are not authorized by this **Policy**

DON'T process purchasing of operating-type goods or capital equipment through expense report unless specifically authorized by Finance Department

DON'T proceed with domestic air travel without pre-approval from direct supervisor or manager

DON'T make travel arrangements less than 5 days prior to travel without justification

DON'T travel First Class under any circumstances (never permitted)

DON'T use indirect routing to increase flight-time to be entitled to fly in next level of class service

DON'T downgrade class of service to purchase tickets for family members when traveling in business class

DON'T include unused airline tickets with Expense Reports unless approved by EX Level executive

DON'T book suites, executive floor rooms, or double rooms (only standard single rooms approved)

DON'T book flights or hotels that cost **Digital Edge** additional money or delay traveler to accumulate affinity points

DON'T claim reimbursement for membership fees associated with reward programs

DON'T use rental vehicles for one-way trips without awareness of potentially high drop-off charges

DON'T take extended medical insurance offered by rental agencies (**Digital Edge**'s medical insurance covers employees)

DON'T use personal vehicles for business trips if reimbursement mileage expense will exceed airline ticket and/or automobile rental expense

DON'T claim mileage for commuting to work from home (only business trips exceeding normal commuting distance)

DON'T claim mileage reimbursement if you receive monthly car or transportation allowance (depending on contract terms)

DON'T claim in-room refreshment (mini-bar) for any item other than water

DON'T fail to provide receipts towards total amount beyond US$25 per day (may result in denial of reimbursement)

DON'T tip excessively or improperly beyond accepted norm within country

DON'T include personal travel that involves extra expense to **Digital Edge** or interferes with business objectives

DON'T incur expenses for spouse or family members traveling with you on business trips (food, lodging, transportation)

DON'T pay and seek reimbursement for travel-related expenses of customer or business partner

DON'T provide gifts, meals, travel, or entertainment to government, quasi-government, or government-affiliated entities (governed by Anti-Bribery Anti-Corruption **Policy**)

DON'T expense meals or entertainment without clear business connection with **Digital Edge**

DON'T submit expense claims for business entertainment without full list of attendees, titles, Company names, and reason

DON'T fail to attach receipts for ALL entertainment expenses

DON'T submit expense claim authorized by approved signatory in attendance at function

DON'T claim gift cards, merchandise (iPads/iPhones), raffle tickets, cash or cash equivalents (gold, jewelry, watches), or charitable donations as gifts or entertainment expenses

DON'T claim gifts that do not meet requirements under Business Code of Conduct, Gift & Entertainment **Policy**, FCPA/ABC legislation, or local laws/regulations

DON'T claim reimbursement for gift cards (not allowed due to tax implications)

DON'T claim membership dues to more than one technical or professional organization

DON'T submit expense reports with incomplete information or missing receipts

DON'T submit expense reports more than 30 days after completion of trip without written explanation

DON'T fail to notify manager or Finance Department of cashflow issues when incurring expenditure on own account

DON'T incur non-reimbursable expenses (see Annexure II for comprehensive list)

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What is the scope of this Policy and who is responsible for compliance?

A: This **Policy** applies to **Digital Edge** and its direct and indirect subsidiaries (collectively, **Digital Edge**) and provides standards and procedures for incurring and seeking reimbursement of authorized expenses. Managers are responsible for ensuring **Policies** and procedures are understood and followed by employees under direct supervision, determining whether each business trip is essential, limiting number of personnel traveling to those necessary, and reviewing expenses to ensure compliance. Employees are responsible for complying with **Policies**, controlling costs, submitting accurate reports, and paying for personal expenses.

Q2: What are the travel approval requirements?

A: **International Travel:** All international travel requires prior written approval from the employee's direct supervisor and Director Level executive to which he or she reports. The same supervisor/executive should review the employee's Expense Reports and submit for reimbursement in accordance with **Digital Edge**'s Expense Approval Process. **Domestic Travel:** Domestic air travel requires pre-approval from the employee's direct supervisor or manager. Request for all travel approval should be submitted using the Pre-Travel Authorization Form.

Q3: What are the authorized airline class of service standards?

A: Authorized airline class of service is determined by an employee’s grade and the duration of the flight, which is calculated based solely on actual airtime excluding layovers. First Class travel is never permitted under this **Policy**. Only CEO or CFO are entitled to make exceptions to Authorized Class of Travel, and such exceptions must be documented in writing and attached to expense report. Only actual airtime as estimated by airline should be used when calculating flight time (layovers and time spent in airports waiting for connecting flights cannot be used).

Q4: What are the accommodation standards and reimbursable lodging expenses?

A: Accommodation is generally reimbursable for business travel exceeding a 150-kilometer radius from your home or work location, though a 100-kilometer threshold applies in Japan. Employees may also be reimbursed for accommodation within a lesser distance if special circumstances would justify an overnight stay. Employees should book standard single rooms in reasonably priced hotels, ideally at corporate rates, and are only permitted room upgrades if provided at no cost. Laundry expenses are reimbursable for stays of three or more consecutive nights. If staying with friends or family instead of a hotel, a token gift for the host up to US$50 per night (totaling no more than US$250) may be expensed.

Q5: What are the automobile rental and personal vehicle reimbursement rules?

A: **Automobile Rental:** All associated costs of rental, gas, and insurance are reimbursable. Mid-size cars are the standard for all employees traveling on **Digital Edge** business. Full size cars can be used if 3 or more employees are riding together. Employees should inspect vehicles for any damage prior to leaving car rental lot. Rental cars are to be returned with full tanks of fuel to minimize refueling surcharges. Each traveler should take Liability and Collision insurance offered by rental Company. It is recommended NOT to take extended medical insurance offered by rental agency (**Digital Edge**'s

medical insurance covers each employee). **Personal Automobile:** Personal vehicles may be used for business trips if reimbursement mileage expense will not exceed airline ticket and/or automobile rental expense. Employees must have sufficient automobile liability and property damage insurance coverage. Employees will be reimbursed on per mile/kilometer rate established locally or as published each year by local government as deductible mileage allowance. Check with Finance Department to ascertain current reimbursement amount in your location. Mileage is not paid for commuting to work from home. Only business trips that exceed normal commuting distance are reimbursable and only for mileage more than normal commuting distance. Employees who receive monthly car or transportation allowance may not be eligible to claim reimbursement for mileage and other car expenses (depending on contract terms).

Q6: What are the personal meal reimbursement requirements?

A: Personal meal expenses are reimbursable for employees on overnight business travel at reasonably priced establishments. All claims must be supported by itemized original receipts; credit card slips alone are insufficient, and missing receipts for daily expenses over US$25 may result in denial. Please note that mini-bar items, with the exception of bottled water, are considered non-reimbursable personal expenses. Where receipts are not available, employees must provide explanation for expenses. Failure to provide receipts towards total amount beyond US$25 per day may result in denial of reimbursement.

Q7: What are the business meals and entertainment requirements?

A: Business meals and entertainment must be infrequent, non-lavish, and necessary for the conduct of **Digital Edge** business. Such activities must comply with the Gifts and Entertainment **Policy** and involve a bona fide business discussion. Providing any gifts, meals, travel, or entertainment to government, quasi-government, or government-affiliated entity is not allowed by **Digital Edge** and is governed by strict guidelines set forth in **Digital Edge**'s Anti-Bribery Anti-Corruption **Policy** and Gift & Entertainment **Policy**. Required information for expensing meals/entertainment: Date; Name of Guests, their title and Company name; Detailed description of type of expense (dinner, lunch, cocktail, sporting event); Establishment name and location address; Business Purpose; Amount Spent (receipts for ALL entertainment must be attached). Most senior persons attending a function must make payment for the entire event.

Q8: What expenses are non-reimbursable?

A: The Company will not reimburse expenses of a personal nature or those not required for business. Non-reimbursable items include but are not limited to adult entertainment, excessive alcohol, childcare or pet care, personal grooming, cash advances, and gift cards. Additionally, personal event expenses like birthdays or weddings, parking or traffic fines, and personal memberships are excluded from reimbursement.

Q9: How do I submit expense reports and what are the approval/payment procedures?

A: All employees must use **Digital Edge**'s web-based automated expense reporting application to submit expenses for reimbursement within 30 days from the completion of the trip. For instructions on how to access/use this application, refer to Finance Department. Each expense report must include

various aspects including but not limited to the Pre-Travel Authorization Form, appropriate cost center, business purpose, and neatly scanned itemized receipts etc. Expense reimbursements will be directly debited and paid to same account that is on file as employee's primary bank with payroll. Payments will be made in next salary run when **Policy**-compliant expense report is submitted and approved with complete receipts attached by applicable cut-off date.

Q10: What are the consequences of non-compliance with this Policy?

A: You are personally liable for expenses that are not in compliance with all requirements of this **Policy**. If **Digital Edge** pays for or reimburses you for any expense that is not ordinary, necessary, and reasonable or is not a business expense, you may be required to repay **Digital Edge** for expense, or it may be classified as compensation taxable to you. In addition, Disciplinary action up to and including dismissal may be taken, and violations involving tax laws may be referred to appropriate authorities for penalties or fines. If **Digital Edge** discovers violation of any tax laws, it may refer matter to appropriate authorities, which could lead to penalties, fines, or imprisonment or other liability. **Digital Edge** will conduct periodic confidential audits designed to prevent and detect violations of applicable tax laws, this **Policy**, and other **Digital Edge Policies**. Finance Department, in consultation with legal counsel, may perform investigation of **Digital Edge**'s records, books, accounts, and any other evidence required to prevent and detect violations and ensure compliance.

AIRLINE CLASS OF SERVICE STANDARDS

Length of Non-Stop Flight	**VP, C-Suite** **(Internal Grades X3-X5)**	**Director - Senior Director** **(Bands 8-X2)**	**All Other Employees** **(Bands 1-7)**
For all domestic flights	Economy	Economy	Economy
For all international non-stop flights of up to 4 hours	Economy	Economy	Economy
For all international non-stop flights greater than 4 hours (not overnight)	Premium Economy	Economy	Economy
For all international non-stop flights longer than 6 hours and overnight	Business Class	Premium Economy	Economy

Notes:

- First Class travel is never permitted under this **Policy**

- Only CEO or CFO are entitled to make exceptions to Authorized Class of Travel (must be documented in writing and attached to expense report)
- Only actual airtime as estimated by airline should be used when calculating flight time
- Employees must use most direct route between origination and destination points
- Employees not permitted to use indirect routing to increase flight-time to be entitled to fly in next level of class service

---

AUTOMOBILE STANDARDS

Automobile Rental:

- Midsize cars are standard for all employees traveling on **Digital Edge** business
- Full size cars can be used if 3 or more employees are riding together
- Employees should use major rental companies when available

Personal Automobile:

- Personal vehicles may be used for business trips if reimbursement mileage expense will not exceed airline ticket and/or automobile rental expense
- Employees must have sufficient automobile liability and property damage insurance coverage
- Employees reimbursed on per mile/kilometer rate established locally or as published by local government
- Mileage not paid for commuting to work from home
- Only business trips exceeding normal commuting distance are reimbursable

---

BUSINESS MEALS AND ENTERTAINMENT REQUIREMENTS

All business meals and entertainment must meet ALL of the following criteria:

- Entertainment must comply with Gift & Entertainment **Policy**
- Entertainment is directly related to active conduct of business
- Entertainment is directly preceded or followed by substantial and bona fide business discussion
- Entertainment consists of business meals (food and beverage) in place conducive to business discussion and guests are engaged in trade, business, or activity having relationship to **Digital Edge**'s business

Required information for expensing meals/entertainment:

- Date
- Name of Guests, their title and Company name
- Detailed description of type of expense (dinner, lunch, cocktail, sporting event)

- Establishment name and location address
- Business Purpose
- Amount Spent (receipts for ALL entertainment must be attached and included in expense report)

Most senior person attending function must make payment for entire event. Where not possible, expense claim must be authorized by approved signatory not in attendance at function.

EXPENSE REPORT SUBMISSION CHECKLIST

Expense report must include:

- Employee name and Employee Code
- Dates of travel or expense incurred
- Cost Centre
- Purpose of travel or expense
- Cities or locations of travel
- Itemized list of costs by date
- Separate disclosure of VAT, GST, consumption taxes or similar incurred
- Separate listing of lodging, meals, transportation, etc.
- Receipts neatly attached to expense report or scanned into reporting tool
- Pre-Trip Authorization Form (Annexure I) attached to expense report
- Employee's signature approval
- Manager's signature approval
- Signature Approval of Director level executive, where required

Expense Reports should normally be submitted within 30 business days after completion of trip.

REPORTING VIOLATIONS

Digital Edge personnel have an obligation to adhere to this Policy.

If you witness behavior on the part of **Digital Edge** personnel that you believe may represent a violation of this **Policy**, you must promptly report it.

Reports should be made to:

- Country Finance Head (in first instance)
- **Digital Edge**'s Ethics Hotline: whistleblower@digitaledgedc.com
- Compliance Department: vishal.jain@digitaledgedc.com

Internal reporting is important to **Digital Edge**, and it is both expected and valued. **Digital Edge** takes all reports seriously, and every report received will be assessed and, where necessary, appropriate investigation will be undertaken.

Confidentiality of reported violations will be maintained where possible, consistent with need to conduct adequate review and subject to applicable law.

No retribution or retaliation will be taken against any person who has made a report based on reasonably good faith belief that a violation of this Policy has occurred.

AUDITS AND INVESTIGATIONS

Periodic Audits:

In furtherance of this **Policy**, **Digital Edge** will conduct periodic confidential audits. Management team will determine frequency and scope of any periodic audit. These periodic audits are designed to prevent and detect violations of applicable tax laws, this **Policy**, and other **Digital Edge Policies**.

Investigations:

In addition to periodic audits, there may also be individual instances in which **Digital Edge** may wish to investigate a certain matter. In these situations, Finance Department, in consultation with legal counsel / Compliance Department, may perform investigation of **Digital Edge**'s records, books and accounts, and any other evidence required under circumstances to prevent and detect violations of applicable tax laws and to ensure compliance with tax laws, this **Policy**, and other **Digital Edge Policies**.

ENFORCEMENT AND DISCIPLINARY ACTION

Digital Edge will impose discipline on individuals found to have breached this **Policy**, in manner that is fair, consistent, and that reflects nature and facts of violation.

Anyone subject to this **Policy** who violates it may face disciplinary actions up to and including termination of his or her employment for cause and without notice.

Violation of this **Policy** may also violate certain tax laws. If **Digital Edge** discovers violation of any tax laws, it may refer matter to appropriate authorities, which could lead to penalties, fines, or imprisonment or other liability.

CONTACTS FOR GUIDANCE

For questions on expense reporting application access/use:

Finance Department

For questions on current mileage reimbursement amount in your location:

Finance Department

For written pre-approval of miscellaneous Digital Edge expenditure exceeding US$1,500:

Finance Department

For assistance updating bank account for expense reimbursements:

Country Finance Team

For cashflow issues when incurring expenditure on own account:

Your Manager or Finance Department

REMEMBER

This Policy provides standards and procedures for incurring and seeking reimbursement of authorized expenses. You may incur and will be reimbursed for expenses that are authorized in this Policy. If an expense is not authorized by this Policy, you are prohibited from incurring it and, if incurred and reimbursed by Digital Edge, you may be required to repay it and any reimbursement may be classified as taxable compensation to you. Failure to comply with this Policy may result in disciplinary action up to and including dismissal. Expense Reports should be submitted within 30 business days after completion of trip. First Class travel is never permitted. All business meals and entertainment must comply with Gift & Entertainment Policy. Report violations promptly to Country Finance Head or Ethics Hotline.

OUTSIDE DIRECTORSHIP POLICY

This section provides a high-level overview of Digital Edge's Outside Directorship Policy for ease of reference. Employees should refer to the detailed Outside Directorship Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

The Outside Directorship Policy ("**Policy**") outlines the procedures that employees ("**Nominees**") must follow before accepting invitations to join the board of directors of other companies ("**Outside Directorships**"). This **Policy** must be read in conjunction with the Company's Code of Conduct.

The Company recognizes that its Nominees are often invited to serve on external boards. This **Policy** ensures that any such directorships are subject to proper pre-approval, do not create conflicts of interest, and do not detract from a Nominee's ability to perform his/her duties at **Digital Edge**.

POLICY OBJECTIVE

The **Policy** is designed to:

- Establish a clear and transparent pre-approval procedure for all Outside Directorships.
- Ensure Outside Directorships do not compromise a Nominee's ability to satisfactorily perform his/her duties at **Digital Edge**
- Identify, prevent, and manage actual, potential, or perceived conflicts of interest arising from Outside Directorships
- Confirm that the Nominee's representation in any Outside Directorship is consistent with the Company's Code of Conduct, in particular the clauses relating to Conflict of Interest and Concurrent Employment
- Provide a framework for the treatment of remuneration received by Nominees for Outside Directorships
- Maintain the Outside Directorships Registry for governance and oversight purposes
- Provide a mechanism for exemptions and periodic review of approved directorships

Compliance with this **Policy** is a condition of continued employment and/or association with **Digital Edge**. Any breach may result in disciplinary action up to and including termination of employment with **Digital Edge**.

DOs AND DON'Ts

DOs

DO satisfy yourself that the entity extending the invitation (Nominating Entity) is one that you can trust, and in which you can work without reputational damage to yourself or to the Company

DO obtain written pre-approval from the Approving Authority before accepting any Outside Directorship

DO submit a completed Appendix A to the Compliance Department to begin the pre-approval process

DO confirm that the Nominating Entity's values and principles align with the Company's Code of Conduct

DO confirm that the Nominating Entity does not have an existing contractual relationship with **Digital Edge**

DO confirm that the Nominating Entity does not have a quid pro quo expectation (in the form of, but not restricted to, favours, business benefits, and employment) in exchange for the Outside Directorship

DO confirm that the time commitment demanded will not disturb or distract you from your duties and responsibilities at **Digital Edge**

DO disclose whether you will or will not receive remuneration from the Nominating Entity, and comply with guidelines issued by the Global Head of Human Resources

DO serve in any Outside Directorship in your personal, and not professional, capacity — under no circumstances may you hold yourself out as a **Digital Edge**-nominated representative with respect to the Outside Directorship

DO pay attention to the Nominating Entity's activities, as any activity conducted by anyone affiliated with the Nominating Entity could be imputed to you

DO ensure your activities for any Outside Directorship comport with the Company's Code of Conduct principles

DO inform the Company of any potential or existing conflict of interest between the Company and the Nominating Entity

DO notify the Compliance Department of any changes to the information contained in your approval request form

DO periodically assess your Outside Directorship for any actual or perceived conflicts of interest between your position at **Digital Edge** and the Outside Directorship

DO seek an exemption from the Approving Authority if any specific provision of this **Policy** cannot be complied with

DON'Ts

DON'T accept an Outside Directorship where the Nominating Entity has an existing contractual relationship with **Digital Edge**, without proper disclosure and approval

DON'T accept an Outside Directorship where the Nominating Entity has a quid pro quo expectation in return for the directorship

DON'T accept an Outside Directorship that poses conflicts of interest that cannot be eliminated or effectively managed

DON'T accept an Outside Directorship that may negatively affect your ability to satisfactorily perform your duties at **Digital Edge**

DON'T hold yourself out as a **Digital Edge**-nominated representative with respect to any Outside Directorship

DON'T accept or retain remuneration from an Outside Directorship without complying with guidelines issued by the Global Head of Human Resources

DON'T fail to inform the Compliance Department (immediately if a conflict of interest arises) following acceptance of an Outside Directorship or any change to the information provided

DON'T fail to notify the Compliance Department of any changes to the information provided in your Appendix A approval request

ADDITIONAL POINTERS FOR CEO

CEO must disclose a list of all positions held through an annual declaration to the Company's Board of Managers and shall balance the demands of the role with any approved Outside Directorships. CEO shall ensure that such roles do not interfere with their responsibilities at **Digital Edge**.

CEO cannot approve his/her own Outside Directorship request — approval must be granted by other members of the Compensation Committee.

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: Who does this Policy apply to?

A: This **Policy** applies to all employees ("**Nominees**") and must be read in conjunction with the Company's Code of Conduct.

Q2: What is an Outside Directorship?

A: An Outside Directorship is a position on the board of directors of a Company outside the **Digital Edge** group (the "**Nominating Entity**"). It includes positions in educational /professional bodies, government committees/bodies or organizations, advisory or technology agencies, charities, social organizations, and associations.

Q3: Do I need approval before accepting an Outside Directorship?

A: Yes. All Nominees must obtain written pre-approval from the Approving Authority (the Company's Compensation Committee) before accepting any Outside Directorship. You must submit a complete Appendix A of **Policy** to the Compliance Department to begin the pre-approval process. Approval requests should be sent to vishal.jain@digitaledgedc.com.

Q4: How many board seats am I permitted to hold?

A: You may hold a maximum of three (3) board seats in non-group companies, a maximum of six (6) combined board seats in group companies and non-group companies, and a maximum of three (3) memberships in external panels, advisory groups, boards, or committees in addition to any approved board seat. (REFER **POLICY** 3B2)

Q5: What does the Approving Authority review before granting approval?

A: The Approving Authority (Compensation Committee) must ensure: (i) the Nominee does not exceed the permitted number of board seats and external memberships; (ii) the Outside Directorship does not pose conflicts of interest that cannot be eliminated or effectively managed; (iii) the Outside Directorship does not negatively impact the Nominee's ability to perform his/her duties at **Digital Edge**; and (iv) the Nominee's representation is consistent with the Company's Code of Conduct, based on disclosures made in Appendix A of **Policy**.

Q6: What conflicts of interest must I be aware of in relation to Outside Directorships?

A: You must ensure the Outside Directorship does not create any actual, potential, or perceived conflict of interest with your responsibilities at **Digital Edge**. The Approving Authority must decline approval where conflicts of interest cannot be eliminated or effectively managed. If a conflict arises after acceptance, you must immediately inform the Compliance Department at vishal.jain@digitaledgedc.com.

Q7: Can I receive remuneration for an Outside Directorship?

A: Any remuneration offered to a Nominee for an Outside Directorship is subject to guidelines issued by the Company's Global Head of Human Resources. You must declare whether you will or will not receive remuneration in approval request and set forth remuneration details if applicable.

Q8: Are there special requirements for the CEO?

A: Yes. If the CEO is the Nominee, the approval request must be reviewed and approved by the other members of the Compensation Committee (i.e., not the CEO). Additionally, the CEO must disclose a

list of all positions held through an annual declaration to the Company's Board of Managers and must balance the demands of his/her role with any approved Outside Directorships.

Q9: What are my ongoing obligations after an Outside Directorship is approved?

A: Following acceptance, you must: (i) periodically assess your Outside Directorship for any actual or perceived conflicts of interest between your position at **Digital Edge** and the Outside Directorship; (ii) immediately inform the Compliance Department if any conflict of interest arises; and (iii) notify the Compliance Department of any changes to the information provided in your approval request. All approved directorships are recorded in the Outside Directorships Registry maintained by the HR Department.

Q10: What are the consequences of violating this Policy?

A: Any breach of this **Policy** - including accepting an Outside Directorship without prior written approval or failing to disclose a conflict of interest — may result in disciplinary action up to and including termination of employment with **Digital Edge**.

COMPETITION POLICY

This section provides a high-level overview of Digital Edge's Competition Policy for ease of reference. Employees should refer to the detailed Competition Policy available on Digital Edge's website at www.digitaledgedc.com for the complete provisions, guidance, and requirements.

HIGH-LEVEL SUMMARY

The Competition Policy ("**Policy**") reflects **Digital Edge**'s commitment to full compliance with competition laws (also known as antitrust laws) in all countries where it operates.

Competition laws are legal rules aimed at protecting businesses and consumers from anti-competitive conduct by encouraging effective competition, enhanced productivity, innovation, and value for customers. Violating competition laws can result in severe civil fines (up to 10% of global turnover in many jurisdictions), reputational harm, private damage claims, and criminal penalties — including imprisonment — for individual Company Personnel.

POLICY OBJECTIVE

The **Policy** is designed to:

- Summarize the basic principles of antitrust laws and regulations applicable to **Digital Edge**'s business operations globally
- Identify potential competition law risks and problem areas in day-to-day business activities
- Explain how Company Personnel can comply with antitrust laws when dealing with competitors, customers, and suppliers
- Prohibit anti-competitive agreements and concerted practices including price fixing, market sharing, bid rigging, and exchange of commercially sensitive information
- Provide guidance on permissible conduct at trade association meetings
- Set out the rules governing relations with customers, suppliers, and competitors
- Address the specific restrictions on companies in a dominant market position
- Summarize the consequences of violating antitrust laws, including civil fines, reputational harm, and criminal penalties
- Establish a framework for reporting, investigation, and enforcement of competition law compliance

Compliance with this **Policy** and all applicable competition/antitrust laws is a condition of continued employment and/or association with **Digital Edge**. Any violation may result in disciplinary action up to and including termination of employment, as well as personal civil and criminal liability.

DOs AND DON'Ts

DOs

DO comply with all applicable competition/antitrust laws in every jurisdiction where **Digital Edge** operates

DO take responsibility for understanding what you and your teams need to do to comply with competition laws

DO use the guidance provided under this **Policy** and associated training to identify and avoid competition law risks in your role

DO seek guidance from your manager and/or the Compliance Department vishal.jain@digitaledgedc.com) if you are in any doubt or have any questions about competition law compliance

DO bid independently and without coordination with competitors in all tender and procurement processes

DO ensure that trade association meetings have a proper antitrust **Policy**, guidelines, and agenda in place before attending

DO keep minutes of trade association meetings and report immediately to the Compliance Department any incident that could have potential antitrust law consequences

DO object immediately to any anti-competitive discussion at a trade association meeting or industry event, and leave the meeting if the discussion continues

DO consult the Compliance Department before entering into any tying or reciprocal buying arrangement with customers or suppliers

DO consult the Compliance Department before any transaction or conduct in markets where **Digital Edge** holds or may hold a dominant position

DO report any known or suspected competition law violations to the Compliance Department or through the Whistleblower reporting channels

DO complete mandatory competition law training and certification within the notified timeframe

DO deal with customers and suppliers fairly and in a manner that best advances the competitiveness of **Digital Edge**'s services

DO ensure that customers are free to independently determine their commercial strategy and freely choose the services or products they purchase

DON'Ts

DON'T engage in any agreement or concerted practice — whether written, oral, formal, or informal — that restricts or aims to restrict competition

DON'T fix, coordinate, or agree prices, discounts, or pricing strategies with competitors (price fixing)

DON'T agree with competitors to divide or allocate markets, territories, or customers (market sharing/allocation)

DON'T coordinate bids or tenders with competitors, or agree that one competitor will be a lower bidder in any procurement (bid rigging)

DON'T exchange confidential or commercially sensitive information with competitors, including pricing, credits, discounts, terms of sale, commercial strategies, identity of customers/suppliers, or details of business partner negotiations

DON'T passively listen to or remain in a meeting where anti-competitive information is being exchanged — the mere receipt of such information can be illegal

DON'T participate in boycotts with competitors, including agreements not to sell to certain customers, joint refusals to buy from suppliers, or agreements not to deal with certain companies

DON'T engage in tying arrangements (conditioning sale of a product/service on the customer purchasing a second product/service) or reciprocal dealing without Compliance Department clearance

DON'T engage in conduct that may constitute abuse of a dominant position (including price discrimination, exclusivity, refusal to supply, predatory pricing, or tying/bundling) without Compliance Department clearance

DON'T retaliate against anyone who reports a suspected competition law violation in good faith

FREQUENTLY ASKED QUESTIONS (FAQs)

Q1: What are competition/antitrust laws?

A: Competition laws (also known as antitrust laws) are legal rules aimed at protecting businesses and consumers from anti-competitive conduct. They prohibit agreements or concerted practices that restrict competition, abuse of a dominant position, and other practices that harm competitive markets, including agreements that may be inferred from conduct. They apply to all of **Digital Edge**'s global operations, and violations can result in fines, civil damages, and criminal penalties.

Q2: What is price fixing and why is it prohibited?

A: Price fixing occurs when competitors make agreements — whether written or oral, formal or informal — to fix trade prices, for example through agreements on discounts. Price fixing is one of the most serious breaches of antitrust laws and is regarded as a cartel, punishable by the highest levels of fines. It is also a criminal offence punishable by imprisonment in many jurisdictions.

Q3: What is bid rigging?

A: Bid rigging involves coordinating tenders or bids between competitors. This includes agreeing that one competitor will be a lower bidder in a procurement, submitting cover bids to make a pre-selected winner appear competitive, or rotating winning bids among competitors. Bid rigging is a serious infringement of antitrust law and a criminal offence in many jurisdictions. Competitors must always bid independently.

Q4: What information can I share with competitors?

A: It is not permissible to exchange confidential or commercially sensitive information with competitors that may reduce or remove uncertainty about current or future market conduct, including through informal discussions, emails, or meetings. This includes pricing, credits, discounts, terms and conditions of sale, commercial strategies, identity of customers and suppliers, and details of negotiations with business partners. Importantly, the mere receipt of such information can be illegal, even if you do not reciprocate.

Q5: What should I do if anti-competitive topics are raised at a trade association meeting?

A: You must object immediately and clearly to any anti-competitive discussion at a trade association meeting or industry event. If the discussion continues, you must leave the meeting, ensure your objection is noted in the minutes, and immediately report the incident to the Compliance Department. Passively listening to anti-competitive exchanges is sufficient to breach antitrust laws.

Q6: What is abuse of a dominant position?

A: Antitrust laws impose specific restrictions on companies that hold a dominant position in a market (generally considered to be a share of 40% or above, depending on market conditions such as barriers to entry and competitor strength). Potentially abusive conduct includes price discrimination, fidelity discounts or exclusivity, refusal to supply, excessive or predatory pricing, and tying or bundling. Any

conduct in markets where **Digital Edge** may be dominant must be cleared with the Compliance Department before proceeding.

Q7: What are the consequences of violating competition laws?

A: Violations can result in: (i) civil fines against the Company of up to 10% of global turnover in many jurisdictions; (ii) private damage claims by affected parties; (iii) reputational harm; and (iv) criminal penalties for individual Company Personnel, including imprisonment, in countries such as Australia, Brazil, Canada, Chile, Israel, Japan, Mexico, the Netherlands, the UK, and the US. The Company cannot defend you against an antitrust violation, and you would bear such costs yourself.

Q8: How do I report a suspected competition law violation?

A: You must report any known or suspected violation to the Compliance Department at vishal.jain@digitaledgedc.com or through the Whistleblower **Policy** reporting channels. **Digital Edge** enforces a zero-tolerance, non-retaliation **Policy** that protects employees who raise concerns in good faith. Potential antitrust law violations are aggressively investigated and strictly enforced.

Q10: Who should I contact if I have questions about this Policy?

A: Contact the Compliance Department for any questions about this **Policy**, antitrust laws, or guidance on a specific issue that might raise competition law concerns. Always seek guidance before proceeding with any transaction or conduct that may present a competition law risk.
