legal@tbdistr.com
www.tbdistr.com

TECHBRIDGE GROUP
CORPORATE COMPLIANCE PROGRAM

legal@tbdistr.com
www.tbdistr.com

Preliminary Notice:

The term "TechBridge" or 'Group" stands for all entities within the TechBridge Group and affiliated companies.

For reference the word "Employee(s)" in this Corporate Compliance Program includes all employees including members of the Board of Management as well as Managing Directors of all entities within TechBridge.

I. COMPLIANCE STATEMENT

TechBridge is dedicated to maintaining excellence and integrity in all aspects of its operations and its professional and business conduct. Accordingly, TechBridge is committed to conformance with high ethical standards and compliance with all governing laws and regulations of the countries where it operates, not only in the distribution scope but in its business affairs and its dealings with employees, administrative staff, counterparties and partners. We have a 'zero tolerance' to illegal and unethical business behavior and activities, including bribery and corruption, money laundering, terrorism financing, economic sanctions circumvention, tax evasion, forced labour and other breaches of human rights. It is the personal responsibility of all who are associated with TechBridge to honor this commitment in accordance with the terms of the TechBridge Group Code of Conduct and related policies, procedures and standards developed by TechBridge. Our Corporate Compliance program defines our principles for conducting business and as such all of our business partners must comply with this as part of their contractual arrangements with TechBridge.

II. PURPOSE OF COMPLIANCE PROGRAM

The TechBridge Corporate Compliance Program (the "Program") is intended to provide reasonable assurance that TechBridge:

1. Complies in all material respects with all federal, state and local laws and regulations that are applicable to its operations;
2. Detects and deters criminal conduct or other forms of misconduct by officers, employees, counterparties, agents and contractors, partners that might expose TechBridge to any civil liability;
3. Promotes self-auditing and self-policing, and provides for, in appropriate circumstances, voluntary disclosure of violations of laws and regulations;
4. Establishes, monitors, and enforces high professional and ethical standards.

This Program establishes a framework for legal and ethical compliance by TechBridge and the members of the TechBridge workforce community. The Program is a living document and all members of TechBridge workforce are encouraged to suggest changes or additions to the Program.

III. SCOPE OF COMPLIANCE PROGRAM

The provisions of the Program apply to all business and legal activities performed by TechBridge's employees, as well as business and financial partners, agents, customers and contractors and other third parties acting on behalf of engaging in any business relationships with TechBridge ("Third Parties"). The expectations for TechBridge's employees regarding compliance with the Program are as follows:

1. Comply with the Group's mission statement and the TechBridge Group Code of Conduct and Corporate Compliance Program;
2. Familiarize themselves with the purpose of the Program;
3. Perform their jobs in a manner which demonstrates commitment to compliance with all applicable laws and regulations;
4. Report known or suspected compliance issues to anyone of competent authority:

- The Compliance Officer
- Immediate supervisor
-General Manager / Chairman / Director / Managing Director of one of the TechBridge's company;
- Human Resources Department;

5. Strive to prevent errors and provide suggestions to reduce the likelihood of errors.

IV. KEY ELEMENTS OF THE COMPLIANCE PROGRAMME:

The key elements of the TechBridge's Compliance Program include the following:

1. Risk based approach:
   - Identifying the risks facing the Group and those presented by each business and financial partners, agents, customers, contractors, government officials or other third party engaging in any business relationships with the Group and taking a considered risk-based approach to elimination and managing them.
   - Undertaking the appropriate Due Diligence on its business partners having regard to the risks that may have been identified in each case.
2. Staff awareness and training

   Ensuring Employees are aware of the compliance risks facing the Company, their obligations and liabilities under applicable laws and regulations, Group's procedures for undertaking customer's and business partner's Due Diligence and how to recognize and report any suspicious activity.

- Identity our customers and business partners (and their Beneficial Owners) and understand their source of wealth and funds.
- Take account of any vendor, government, regulatory and international findings concerning blacklisted countries and persons and check that TechBridge's customers and business partners are not subject to any blocks.

3. Prohibited business

   We cannot accept businesses which sell illegal products or are involved in any illegal activity.

- In any way that breaches any applicable local, national, or international law or regulation, or causes TechBridge to breach any applicable law or regulation;
- In any way that is unlawful or fraudulent, or has any unlawful or fraudulent purpose or effect;
- For the purpose of harming or attempting to harm minors in any way;
- For anything that is abusive, harmful, or does not comply with our content standards;
- For any unsolicited or unauthorised advertising, promotional material, or any other form of spam;
- To deal in harmful programs such as viruses, spyware, or similar computer code designed to adversely affect the operation of any computer software or hardware;
- In any way that would locally or internationally evade any applicable taxes or facilitate tax evasion.

  TechBridge will not commence any business relationship unless the Customer and Business partner Due Diligence has been completed.

V. CORRUPTION

We conduct ourselves and our work in an honest and fully transparent way to avoid even the appearance of corruption. Corruption is a form of dishonesty or a criminal offense which is undertaken by a person or an organization which is entrusted in a position of authority, in order to acquire illicit benefits or abuse power for one's personal gain. Corruption may involve many activities which include bribery, influence peddling and embezzlement and it may also involve practices which are legal in many countries. Corruption can lead to legal penalties and damage to the reputation of TechBridge.

VI. BRIBERY AND KICKBACKS

Bribery refers to the offence of promising, offering or granting, either directly or indirectly, a person to either perform or to omit an act that is included in their duties or constitutes a violation of their duties. Bribery includes a public official (including foreign public officials and employees of international organizations), or a manager/employee of any capacity in an organization in the

private sector, directly or indirectly demanding, accepting or receiving, an undue gift, benefit or grant in order to perform or omit from performing an act within or in breach of the duties of their office.

TechBridge is committed to conducting its operations in the countries where we do business ethically and in compliance with all applicable laws. As part of this commitment, it is important that we act with integrity in all that we do. Vigilance in complying with all applicable anti-corruption and anti-bribery laws and regulations that aim to prevent Bribery and Corruption is critical as TechBridge conducts increasingly more Global business. TechBridge does not request, require, accept or offer bribes of any kind.

Kickbacks are a form of bribes. Giving or receiving bribes/kickbacks is illegal and can severely damage our reputation.

Bribery in both the public and private sectors, the recipient of the bribe, the offeror of the bribe as well as any facilitator acting as a mediator or contact between the recipient and offeror could all face legal consequences.

Special vigilance is required with respect to international corruption and bribes and you must report any suspicious circumstances.

General Requirements to prevent Bribery and Corruption.

1. Employees and Third Parties (if acting on behalf of TechBridge) may neither directly nor indirectly offer, pay, seek, accept, promise or authorize any financial or non-financial advantage to any government official, other person or entity (including those in the private or commercial sector) as well as charities or non-profit organizations that may be associated with government officials, other persons or entities, with the purpose to influence a business outcome improperly, induce or reward improper conduct, induce the counterpart to take (or to refrain from taking) action or influence any commercial, contractual, regulatory or personal decision. This would be qualified as Bribery or Corruption.
2. Financial and non-financial advantages include, but are not limited to:

– Cash
– Cash equivalents, such as gift cards, vouchers, loans
– Gifts, Entertainment or Hospitality
– Charitable Donations
– Educational, employment or other valuable opportunities

3. Employees and any Third Parties acting on behalf of TechBridge are strictly prohibited to pay or offer to pay anyone facilitating payments to speed up or secure a routine government activity, such as customs clearance, visa processing or securing the performance of otherwise routine governmental action. Paying facilitating payments could have a serious

impact on the reputation of TechBridge and could result in penalties or prison sentences for anyone who would engage in such practices. If asked to pay a facilitating payment, such requests have to be denied and reported to the Compliance Officer.

4. Payments that TechBridge is prohibited from making directly under this Program cannot be made indirectly on behalf of TechBridge by any Third Party. Since anti-corruption and anti-bribery laws prohibit indirect as well as direct payments and offers, employees and/or TechBridge may be held liable for the conduct of Third Parties.
5. Commissions, rebates, sales discounts, bonuses and other similar payments should be paid in accordance with properly established accounting and finance procedures. Employees and Third Parties must never make any side payments or any other unauthorized use of funds of TechBridge. For a bribe to be paid the funds may have been taken from our company; if we can stop the flow of corrupt payments, we can prevent Bribery and Corruption in many cases. Any requests for additional bonuses, discounts or other payments must be properly authorized and documented.

VII. MONEY LAUNDRING AND TERRORIST FINANCING

Anti-Money Laundering (AML) consists of regulations and laws that deter the movement and washing of illegal funds. For example, AML measures target terrorist financing, tax fraud, and international smuggling.

Article 6 The United Nation office for Drug Control and Crime Prevention defines “Money Laundering” as:

- The conversion or transfer of property for the purpose of concealing or disguising the illicit origin of such property or of assisting any person who is involved in the commission of the predicate offence to evade the legal consequence of his or her actions;
- The concealment or disguise of the true nature, source, location, disposition movement or ownership of property;
- The acquisition, possession or use of property by any person who knows, suspects, or should have known that such property, was derived from crime as defined by the member states.

International Monetary Fund (IMF), describes Money Laundering as ‘the process by which a person conceals or disguises the identity or the origin of illegally obtained proceeds so that they appear to have originated from legitimate sources.”

Be wary and report of the following “red flags” that may indicate money laundering or other corruption:

- Technological features that increase anonymity - such as the use of peer-to-peer exchanges websites, mixing or tumbling services or anonymity-enhanced cryptocurrencies.
- The counterparty tries to conceal its identity or the source of its funds.

- The counterparty is an entity without a clear registered office and does not appear online.
- The counterparty's structure makes it difficult to recognize it.
- Documents that cannot be verified.
- Multiple tax ID numbers.
- Reluctance to provide detailed information about the business.
- Shielding the identity of beneficial partners or owners.
- The counterparty funds for the transaction come from abroad when there is no apparent link between the country where the funds are sourced and the third party.
- The counterparty uses multiple bank accounts or ones held abroad without any justification.
- The counterparty intends to make payments in cash or using bearer checks.
- The counterparty intends to pay a higher price for the services for no good reason.
- The counterparty is based in a tax haven or a high-risk country.

The careful examination of those operations where risk factors exist is essential. TechBridge and its employees should not initiate, maintain or accept a new business relationship (customer, supplier, financier, etc.), provide services or act with anyone known or suspect to be involved in money laundering or terrorist financing, even if in different businesses from the relationship being established with TechBridge. Employees should not deal with money, goods, or valuables that they are aware of or suspect to be from an illicit origin or that they are unaware of. The AML Law of all countries where TechBridge operates designates money laundering and terrorism financing as a criminal offence.

Consequences of Non-Compliance

1. Falling to report - Employees who are aware of any offence occurring withing their establishments relating to money laundering, terrorism and terrorism financing yet refrain from notifying competent authority in TechBridge shall be subject to disciplinary action.
2. Tipping off - employees are specifically advised that they may face a criminal penalty if they fail to report suspicions of money laundering or if they "tip off" a person from disclosing directly or indirectly to the customer or to any other person that they have reported or are intending to report the suspicion transactions.
3. TechBridge and any of its employees may be criminally liable for the offence of money laundering if such an activity is committed from its name or from its account and they may also face the administrative fines and enforcement action in case of a breach any provision of the AML Law or the implementing Program thereof.

VIII. TAX COMPLIANCE AND RELATIONSHIP WITH TAX AUTHORITIES

The purpose of this section is to set out our approach to managing tax compliance and our relationship with tax authorities. For the purposes of this Program, "tax compliance" means

compliance with tax legislation, regulations, protocols and rulings, Tax filing requirements, Transfer Pricing filing requirements, Indirect Tax filing requirements and tax payment obligations of the respective country.

TechBridge is committed to complying with tax laws in all countries in which we operate. The positions taken in TechBridge tax returns are supported by relevant tax law. Where the law is subject to different interpretations, we seek appropriate advice. We take advantage of government concessions within the spirit they are intended.

When the application of sound judgement is required, it is taken by appropriately qualified tax professionals within a collaborative environment of consultation with the business. We employ appropriately trained tax professionals in the countries where we have material economic activities.

Tax risks are identified, evaluated and accounted for appropriately. We continually seek to improve processes for assessing, recording, and reporting of tax risks to ensure transparency and appropriate decision making to manage risks. Our tax planning is based on interpretations of the law and is aligned with the substance of the economic activity. Where there is significant uncertainty or complexity in relation to tax risk external advice is sought.

We prepare and file all tax returns on time and make all tax payments on time in compliance with the Tax Laws of the respective country. As a company we ensure the company's tax positions are in alignment with Tax laws and guidelines issued by the Tax Authorities. As a company we also ensure that our documentation is robust and up to date and shall maintain all records and documents for a minimum period of seven years, or as dictated by national tax law if longer, following the end of the Tax period.

Relationships with Tax Authorities

We seek to build and sustain our relationships with governments and revenue authorities in an honest, respectful and constructive way. We never intentionally mislead any government official or attempt to conceal, alter, or destroy documents, information or records that are required to be held by law.

IX. INTEGRITY OF RECORDS AND COMPLIANCE WITH ACCOUNTING PROCEDURES

Accuracy and reliability in the preparation of all business records is mandated by law. It is of critical importance to the corporate decision-making process and to the proper discharge of TechBridge financial, legal and reporting obligations. All bills rendered to partners, their representatives or third parties must accurately reflect the services provided, and the partners' records shall properly and accurately record those services. All business records, expense accounts, vouchers, payroll and service records and other reports are to be prepared with care and honesty. False or misleading entries are not permitted to be recorded in the books and records of

TechBridge. All corporate funds or assets are to be recorded in accordance with applicable corporate procedures. Compliance with accounting procedures and internal control procedures is required at all times.

We seek to comply with legislation requirements regulating Ultimate Beneficial Owner (UBO) Procedures. All company secretarial records regarding UBO are to be prepared carefully and honesty and report on time if required.

All responsible employees shall maintain an effective system of internal accounting controls including periodic audits. Audits may be performed by management, government agencies, Internal Audit and external financial auditors. Employees must cooperate with auditors and provide information that is truthful and accurate.

It is the responsibility of all employees to ensure that both the letter and the spirit of corporate accounting and internal control procedures are strictly adhered to at all times. Any employee should advise competent authority and the Corporate Compliance Officer of any shortcomings they observe in such procedures.

X. ECONOMIC SUBSTANCE

We seek to compliance with Economic Substance requirements in relation to TechBridge activity:

- TechBridge entities conduct ‘core income-generating activities’ within the Country of tax residence;
- TechBridge entities direct and manage business from within the Country of tax residence;
- TechBridge entities employ adequate full-time staff in the Country of tax residence;
- TechBridge entities incur adequate operating expenditure in the Country of tax residence; and
- retain adequate physical assets in the Country of tax residence as per local laws.

All TechBridge’s information and records demonstrating the economic content of TechBridge business activities are to be prepared carefully and honesty and report to the regulatory authorities within appropriate timelines.

XI. ECONOMIC SANCTIONS

TechBridge operates in accordance with all applicable economic restrictions and complies with the terms of all international sanctions law applicable to our business activities. These include the laws and regulations administered by the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC), the U.S. Department of Commerce’s Bureau of Industry and Security (BIS), the European Union, the United Nations or it’s Security Council as well as similar laws and regulations in other jurisdictions (hereinafter referred to as International sanctions). Compliance with existing international sanctions is one of the most important conditions for complying with the Group’s high standards in professional, ethical and other areas which include:

- Screening counterparties and transactions against global sanctions and Specially Designated National lists issued by the United Nations Security Council (UNSC), the European Union (EU), the United States (OFAC) and any other local national sanction lists that may be appropriate.
- Prohibited business activity which includes on-boarding or continuing customer relationship or providing products or services or facilitating transactions that TechBridge believes may violate applicable sanctions. This includes prohibitions on business activity with individuals or entities named in international sanctions lists or activity, directly, involving countries or territories subject to national or vendor sanctions.
- TechBridge will not deal directly or indirectly with any person/entity that may result in a violation of any national sanctions regulations.
- The Company undertakes not to conduct business in countries that are under any sanctions.

All employees shall look for any red flags or suspicions that may indicate the direct or indirect involvement of a restricted territory, restricted party, controlled item, service, end-use or any other sanctions compliance concern.

Examples of Red Flags to be reported include:

- A lack of information as to the identity of the end-client involved parties and/or the reluctance of a party to provide such information;
- Unusual invoicing requests;
- Unusually favorable payment terms;
- Any suspicion or evidence to suggest the possible involvement of a restricted territory or restricted party.

The examples of Red Flags stated above are not an exhaustive list. Any suspicion of the direct or indirect involvement of a restricted territory or party should alert you to further investigate the activity in accordance with this Program and report it to the Corporate Compliance Officer and competent authority in TechBridge.

XII. TRADE REGULATIONS AND RESTRICTIONS

Complementing the economic sanctions laws, the United States, the Member States of the European Union and many other countries have adopted export control laws that regulate the export and re-export of goods, software and technology to specified destinations and end-users for specified purposes and applications. These laws apply to intra-company transfers as well as to dealings with third parties. Export control laws may prohibit a particular export or re-export of goods, software or technology. Similar to economic sanctions lists, the United States and other countries maintain various export controls lists (e.g., Entity List, Denied Persons List, Unverified Persons, etc.) with varying restrictions.

TechBridge is a distributor of Data Capture, Data Storage, Data Networking, and IT Security products and services. Certain IT products may contain encryption and that such items are subject to specific U.S. and foreign import/export controls.

TechBridge is NOT engaged in any military activities or any nuclear, missile, chemical or biological end use activities and shall not resell the goods purchased or any DEMO/POC loaned to any party engaged directly or indirectly in any military activities or any nuclear, missile, chemical or biological end use activities without an appropriate Export License when applicable.

TechBridge shall not engage in any resale, export or transfer to:

- Any entity / person prohibited by U.S. law from receiving (exports including those listed on the Denied Parties list, the Entity List and the Specially Designated Nationals List https://sanctionssearch.ofac.treas.gov/
- Any entity / person prohibited by European Union law (including those listened in the Annex 1 of the European Council Regulation (EU) No 269/2014 of 17 March 2014 and European Council Regulation (EU) No 833/2014 of 31 July 2014 https://www.sanctionsmap.eu/#/main
- to any entity/Person prohibited by United Nations Security Council Sanctions https://www.un.org/securitycouncil/content/un-sc-consolidated-list
- To or through any of the following territories: Cuba, North Korea, Iran, Syria, the following parts of Ukraine: Crimea, Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR) or any other territory embargoed by the vendor, appropriate Nation State, US or EU from time to time.

XIII. DEU DILIGENCE AND KYC PROCEDURES

TechBridge is committed to fighting against money laundering, the financing of terrorism, bribery, sanctions circumventing and other illegal issues. The following due diligence principles and KYC procedures are followed, not only in situations where particular risk factors exist, but as to all counterparties and third parties:

Identifying the Counterparty

TechBridge must conduct due diligence on counterparties and other third parties and document the findings. As part of the due diligence process, the following minimum information should be collected:

- Full legal name of the company and its partners with more than 10% of participation or full legal name of the individual;
- legal and actual address (utility bill or other bank statements from the previous three months);
- Memorandum and Articles of Association;
- Trade License or Certificate of Incorporation;
- Documents confirming the authority of the representative.

Also, if deemed necessary, TechBridge can request additional information in order to better assess and mitigate integrity and money laundering risks including information about affiliates and beneficial owners of the entity.

As part of due diligence, TechBridge must verify that the counterparty or third party does not appear on any of the US Department of the Treasury Office of Foreign Assets Control's sanctions list, including the Specially Designated Nationals and Blocked Persons lists, as well as on any Annexes of the Sanction Regulations of the EU Commission (including Annex 1 of the EU Council Regulation 269/2014 from 17 of Match 2014) and the United Nations Security Council (UNSC) sanctions resolutions on the linked Internet websites provided above.

Please note that these lists are revised and updated periodically. Therefore, it is essential to consult the lists at the time of the proposed transaction.

TechBridge should ask and search to confirm whether the client or third party is or has been involved in an investigation of any kind involving corruption, money laundering or acts of terrorism. TechBridge will not enter into a business relationship with a person or an entity that appears on one of these lists.

If you are unsure whether enhanced due diligence is required in a particular situation or have any other questions regarding enhanced due diligence, you should contact Corporate Compliance Officer.

XIV. REPORTING MECHANISMS

One of the key ingredients of an effective Compliance Program is the development of a system which employees can use to report questionable behavior without fear of retaliation. Anyone should make a report in case:

- A breach of employee confidentiality by a co-worker;
- Accepting bribes or kickbacks from a vendor or other third party;
- Any act by any co-worker, business partner, subcontractor, customer, government official or other third party having any business relationships with the Group which may constitute an offence or misdemeanor under the applicable laws (including money laundering, violation of economic sanctions and trade restrictions etc.);
- Unethical or illegal activities by any co-worker;

Any person may submit a notification of any of the above facts without fear of dismissal or retaliation of any kind. Reports may be made verbally or in writing and if preferred anonymously. TechBridge shall make sure that no one who reports an actual or attempted violation to the Program or Code of Conduct is subject to any form of retaliation, illicit conditioning, harassment, or discrimination at the workplace, as a consequence of his/her reporting a violation of the Program, Code of Conduct or of any internal procedure.

Any concerns of the TechBridge's employee, partners, clients or subcontractors may be addressed to:

- Competent Authority - General Manager / Chairman / Director / Managing Director of one of the TechBridge's company;
- The Compliance Officer;
- Employees are expected to bring these types of issues or concerns to their immediate supervisor or directly to Compliance Officer. The supervisor should then evaluate the situation and address it after consultation with the Compliance Officer.

Employees, external business partners, consumers, or anyone else can use the Helpline on our website: https://tbdistr.com/ to speak up about any business or workplace conduct that seems inconsistent with TechBridge's policies, or the law. The TechBridge Helpline provides an anonymous way to report concerns about potential violations.

Employees may feel free to address any concerns also by email for Corporate Compliance issues: legal@tbdistr.com.

When making a report please try to provide as much information as possible to enable the Compliance Officer to research the issue.

Handling of Reported Violations

All reported violations will be acknowledged within five business days by the Compliance Officer, promptly investigated and, if warranted, acted upon with the appropriate corrective action. While some investigations might take longer than others, TechBridge's general practice is to conclude them as soon as practical without compromising the integrity and thoroughness of the necessary investigation. Unless the reported violation is against General manager/Chairman/Director/ Managing director of the TechBridge's company, he/she will be promptly notified of all reported violations. The Audit and Finance department will also be promptly notified and involved in any reported concerns or complaints that involve corporate accounting practices, internal controls, or auditing regardless of origin.

XV. VIOLATIONS TO THE COMPLIANCE PROGRAM & CONCEQUENCES

Compliance with the Compliance Program is an essential part of the contractual obligations undertaken by our employees, temporary workers, independent contractors, and other parties doing business with TechBridge.

The Management of TechBridge is responsible for ensuring that all employees understand and meet the Group's expectations. The Management is responsible for and ensures that the commitments stated in the Compliance Program are implemented in all the Business Units and Corporate functions.

Consequences of Non-Compliance

Non-compliance with the program may result in;

- Criminal or civil actions / liabilities not limited to potential fines and imprisonment under applicable laws and regulations and/or international laws and regulations if applicable;
- Serious reputational damage including media comment;
- Unenforceability of contracts entered into as a result of Bribery, Corruption, fraud or other illegal acts;
- Temporary or permanent loss of current and future opportunities.

For TechBridge Employees

Failure to comply with this Program may lead to disciplinary action up to and including termination of employment. Likewise, as permitted by law, an employee's failure to report known or suspected wrongdoing of which the employee has knowledge may, by itself, subject that employee to disciplinary action up to, and including, termination. Any breach of applicable laws may subject the individual to civil and criminal penalties and/or disciplinary action.