

DataBank Code of Business Conduct and Ethics

Contents

A. Introduction	3
B. Honest and Ethical Conduct	3
C. Compliance with Applicable Laws, Rules and Regulations	3
D. Conflicts of Interest	4
i. Gifts and Entertainment.....	4
E. Corporate Opportunities.....	5
F. Fair Dealing, Antitrust, and Competition	5
G. Confidential Information.....	6
H. Handling External Communications	7
I. Protection and Proper Use of the Company's Assets	7
J. Maintaining Accurate Books and Records	8
K. Retention of Business Records	8
L. Fraud, Anti-Bribery, and Anti-Corruption	9
i. Foreign Corrupt Practices Act (FCPA).....	9
M. Anti-Boycott	9
N. Political Contributions and Interactions with Government	9
O. Employment Practices and Human Rights	10
i. Equal Employment Opportunity	10
ii. Anti-Harassment and Non-Discrimination	10
iii. Anti-Human Trafficking, Forced Labor, and Child Labor	10
iv. Human Rights	10
P. Health and Safety	11
Q. Environment and Sustainability.....	11
R. Reporting Violations (Whistleblower Policy)	11
i. Duty to Report	11
ii. Reporting Procedures	12
iii. Confidentiality	12
iv. No Retaliation.....	12
S. Waivers of or Changes to the Code of Business Conduct and Ethics	13
T. Administration and Implementation	13
U. Other Compliance Policies and Procedures	13
V. Website Disclosure	13

Dear DataBankers:

Our name and reputation are among our most valuable business assets. They represent the trust, integrity, and quality that we have built with our clients, partners, and stakeholders over time. Cultivating and maintaining these assets is essential to our long-term success. Every action we take reflects on our identity and commitment to excellence. We are dedicated to upholding our standards, fostering strong relationships, and consistently delivering exceptional value, knowing that each positive interaction strengthens our reputation. By safeguarding our name and standing in the industry, we ensure sustainable growth and a legacy of trustworthiness for years to come.

As we have all witnessed, years of hard work and integrity by many can be erased overnight by the unethical actions of a few. That is why together, we must make it a priority to uphold our reputation every day in all we do. We must conduct ourselves and hold each other accountable not just to the laws and regulations that apply to our business, but also to the highest principles of business ethics and conduct. This task is fundamental to the continued well-being of our people, our customers, our investors, and all we do business with. That is why we have created this Code of Business Conduct and Ethics (i.e., the “Code”) document, which has been approved by our Board of Directors. The purpose of the Code is to clearly outline the Company’s commitment to an ethical way of doing business. We expect all employees, regardless of title or tenure with DataBank, to uphold the standards outlined in the Code.

Please review it carefully, ensuring you understand the different scenarios and the implications of non-compliance. The Code cannot and is not intended to cover every applicable law or provide answers to all questions that might arise. In some cases, we must rely on each person’s good sense of what is right, including seeking guidance from others on the appropriate course of conduct.

Our name and reputation are among our greatest assets, and each of us plays a vital role in nurturing and upholding them. Please familiarize yourself with the Code and reach out to your supervisor or Human Resources if anything remains unclear.

Raul K. Martynek
Chief Executive Officer

A. Introduction

DataBank Holdings, Ltd., and its affiliates (collectively known as "DataBank" or the "Company"), uphold a general policy of carrying out every business activity and transaction responsibly and with utmost integrity. To implement this general policy on integrity, honesty, and fair play, the Company has adopted the following Code of Business Conduct and Ethics (the "Code"). The Code requires adherence to all laws, rules, and regulations applicable to our operations, but the Code is also designed to ensure that DataBank's ethical standards are built on a broader foundation, reflecting our values and a deep-seated commitment to integrity and fairness. Our goal is to align DataBank's business practices with the provisions of the United Nations (UN) Global Compact and the Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises. Further, this Code supports our corporate values to Put People First, Be Data-Centered, and Inspire Confidence. This Code applies to all directors, officers, employees, and other individuals working for the Company with express authority to act on behalf of DataBank (collectively, "DataBankers"). The Code embodies DataBank's core values, serves as the backbone of our culture, and establishes the fundamental standard to which every DataBanker is held and expected to perform.

As a member of the DataBank family, you are expected to read the Code, apply it to your business responsibilities, behave in accordance with its guidelines, and avoid any impropriety or the appearance of wrongdoing. DataBank maintains exclusive discretion to interpret the terms and conditions of this Code, as well as all other policies concerning the terms and conditions of employment. The Code should not be considered as an employment contract, nor does it promise specific employment privileges or secure employment duration. DataBankers who violate the standards in this Code will be subject to disciplinary action, which may include suspension, termination and/or the reporting of violative conduct to appropriate regulatory and criminal authorities.

If a law conflicts with a policy in this Code, a DataBanker must comply with the law; however, if a local custom or policy conflicts with this Code, a DataBanker must comply with this Code. Any questions about these conflicts or this Code should be directed to DataBank's human resources team ("Human Resources").

B. Honest and Ethical Conduct

As a DataBanker, it is your responsibility to uphold honest and ethical behaviors. You are expected to act with the highest standards of professional integrity and refrain from tolerating anyone who seeks to deceive or avoid responsibility for their actions. All actual or potential conflicts of interest between personal and professional relationships must be handled honestly, ethically, and in accordance with the policies specified in this Code. In addition, all DataBankers must be honest and truthful in discussions with, or requests for information from, the Board, regulatory agency officials and government officials, as well as in all dealings with investors.

C. Compliance with Applicable Laws, Rules and Regulations

DataBankers must respect and obey the laws, rules and regulations of the jurisdictions in which we operate and the rules and regulations applicable to the Company's business. Should you encounter any uncertainty regarding the relevance or interpretation of specific laws, rules, or regulations, we strongly encourage you seek guidance from your supervisor, Human Resources, or DataBank's legal team.

Disregard of the law will not be tolerated. Violation of any applicable laws, rules and regulations may subject an individual, as well as the Company, to civil or criminal penalties. DataBankers should be aware that their conduct and records, including emails, are open to audits and may be discoverable in civil and/or criminal proceedings. This transparency underscores the critical need for ethical, responsible behavior and full legal compliance, reinforcing our commitment to accountability at all stages of our work.

D. Conflicts of Interest

A “conflict of interest” occurs when a person’s private interest interferes in any way (or creates the appearance of interference) with the interests of the Company as a whole. Conflicts of interest also arise when a DataBanker, or any Family Member of such person, receives improper personal benefits as a result of his or her position at the Company. Loans to, other than those made in the ordinary course of business, or guarantees of obligations of, employees or their Family Members may also create a conflict of interest. For purposes of this Code, “Family Member” generally means a person’s spouse, parents, children and siblings, whether by blood, marriage or adoption, or anyone residing in such person’s home.

All DataBankers must avoid any situation in which personal interests conflict, or have the appearance of conflicting, with those of the Company. DataBankers may not accept any benefits from the Company that have not been duly authorized in accordance with DataBank policies. Transactions or arrangements that may involve a conflict of interest are prohibited unless they are sanctioned exceptions to the requirements of the Code as indicated under “Waivers of the Requirements of This Code”.

i. Gifts and Entertainment

DataBank understands that usual business practices occasionally comprise the offering of meals, token gifts, prizes to employees and/or entertainment by or to current or prospective clients, vendors, and business partners in the course of pursuing the legitimate business interests of the Company. This Code and DataBank’s separate Conflicts of Interest and Gifts and Entertainment Policies are not meant to ban such legitimate customary business practices that are designed to create goodwill and enhance business relationships.

Gifts and entertainment to or from third parties must be moderate in value, suitable in nature or otherwise disclosed and authorized as required according to company policy. Exceptions should be rare, approved in advance, and reported to HR (may trigger IRS payroll reporting). This applies for employees, contractors, vendors, and external parties.

Examples of acceptable gifts and prizes include the following:

- Occasional traditional business gifts (not cash) with a low fair market value (less than \$100).
- Occasional parties, group meals, picnics for employees or their guests (in accordance with guidelines on meals and entertainment).
- Flowers, fruit, books or similar provided to employees under special circumstances (for example, on account of illness, or family crisis).

In line with DataBank’s commitment to conducting our business with honesty and integrity and the Company’s policy prohibiting any undisclosed actual or potential conflicts of interest, the following forms of gifts or entertainment are prohibited:

- Gifts of cash equivalents (i.e. gift cards) over \$100 — whether given or received.
- Gifts or entertainment that might reasonably be interpreted as a bribe or a payoff.
- Gifts or entertainment intended to sway business with a person or an entity they are affiliated with; and

- Gifts or entertainment that are illegal, obscene, or offensive in nature or would embarrass DataBank if made public.
- Gifts to individuals, not connected with business purposes (e.g., year-end holiday or birthday gifts).
- Merchandise, company branded items, prizes or gifts valued at large dollars amount (>\$100).

DataBank employees are also discouraged from requesting a favor, gift, or entertainment from vendors, suppliers, customers, and other third parties. If there is doubt over whether it is suitable or acceptable to give or receive a specific gift or entertainment, it is advised to discuss it with your supervisor or management.

DataBank's Conflicts of Interest and Gifts and Entertainment Policies are established to protect both DataBank and each of its employees by preventing even the reasonable semblance of a conflict or inappropriate bias. If any questions arise regarding what gifts and entertainment must be disclosed or which approvals are required under certain circumstances, please seek guidance from your supervisor or the Company's General Counsel.

E. Corporate Opportunities

DataBankers are forbidden from exploiting company property, information, or their role for personal benefit. While serving or being employed by DataBank, all DataBankers must not:

1. Seize corporate opportunities learned through their service or employment with DataBank for themselves or their acquaintances.
2. Utilize company property, information, or their company position for personal benefit during or after service with the company; or
3. Engage in competition with the Company, including but not limited to:
 - a. **Preparing to Compete:** Engaging in any activities that pave the way towards competing with the company while employed, such as planning or organizing a competing business or leveraging company resources or confidential information for competitive purposes.
 - b. **Employment with Competitors:** Simultaneously working or collaborating with a competitor while employed by the company, as this may compromise loyalty, confidentiality, and objectivity.
 - c. **Direct Competition:** Actively engaging in activities that compete with the company's business, including creating or aiming to create a business that offers similar products or services, thereby undermining the company's competitive position.

F. Fair Dealing, Antitrust, and Competition

We seek to outperform our competition fairly and honestly. We seek competitive advantages through superior performance, never through unethical or illegal business practices. Stealing and/or misappropriating proprietary information and/or trade secret information or inducing such conduct by past or present employees of other companies is prohibited. Each DataBanker should endeavor to respect the rights of, and to deal fairly with the Company's customers, suppliers, consultants, competitors, employees and other persons with whom the Company transacts business. No DataBanker should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair dealing practice.

Antitrust laws are designed to foster a free-market economy and stimulate competition. These laws can be intricate, but broadly speaking, they forbid competitors from entering into agreements that could be perceived as a restraint on trade or an attempt to diminish or eliminate competition. DataBank has and always will, gain its edge in the industry by adhering to its fundamental principles and not through potential illegal or unethical acts. Therefore, it is critical to keep these laws in mind before concluding any agreement or even sharing information with DataBank's rivals. Violating these laws can lead to serious repercussions for DataBank and its employees, encompassing both civil and criminal penalties for those implicated. If you have any concerns about a proposed course of action and its potential repercussions under U.S. or international antitrust laws, you should consult with the DataBank General Counsel or a member of the Compliance team for direction.

G. Confidential Information

During the course of work, DataBankers may come across information or learn facts about the Company's business, plans, operations, or the business of DataBank customers that are not known to the general public or to competitors. This type of information is deemed confidential and stands as one of DataBank's most treasured resources. Confidential information is vital to DataBank's prosperity and can come in varied forms such as technical, strategic, operational, financial, and other non-public business details. Making this confidential information known beyond DataBank can place the Company at risk by offering our rivals a glimpse into DataBank's functions and/or strategic objectives, thus granting an unfair competitive advantage to these competitors.

Every DataBanker has the responsibility to handle DataBank's confidential information carefully, aiming to avert any unintended or accidental exposures. The phrase 'confidential information' denotes, but is not restricted to:

- Company Financial Information.
- Marketing Strategies.
- Pricing.
- Customers and Potential Customers.
- Suppliers.
- Skills and Abilities of Personnel.
- Trade secrets.
- Intellectual property.
- Technical materials and information.
- Growth strategy and Capital Plan.
- Bid data, acquisition and divestiture activities, counterparty names, and transaction timing and transaction information.
- Processes and technology developed for or used by DataBank.
- Ownership, financing, marketing, and hedging activities.
- Methods of Procedures (MoP) that are used in the operation of DataBank's business or that may be used in the operation of DataBank's business in the future; and
- Other information relating to the DataBank's business that is not public knowledge.

Except as required by law, rule or regulation or as expressly authorized by the Company's Chief Executive Officer or the General Counsel or Human Resources, every who has access to confidential information must limit disclosure of such information to other DataBankers who have a clear need to know such

information. If DataBankers are required by law, rule and/or regulation to disclose confidential information, they should immediately contact the General Counsel or Human Resources.

Confidentiality agreements are commonly used when the Company needs to disclose confidential information to clients, customers, suppliers, distributors, consultants, joint venture participants or others. A confidentiality agreement puts the person receiving confidential information on notice that he or she must maintain the secrecy of such information. If, in doing business with persons not employed by the Company, you foresee that you may need to disclose confidential information, you should engage General Counsel and discuss the necessity or appropriateness of entering into a confidentiality agreement.

Any employee who improperly copies, photograph, records, removes (whether physically or electronically), uses, or discloses confidential information to anyone outside of the Company may be subject to disciplinary action up to and including termination, and may be liable to pay the Company damages caused by such conduct.

DataBankers also have a responsibility to uphold laws around medical information under the Health Insurance Portability and Accountability Act (HIPAA), personal identifiable information, and data privacy which can be found in our Information Security and Data Privacy Policies.

Your obligation to treat information as confidential does not end when you leave the Company. Upon the termination of your employment, you must return everything that belongs to the Company, including all documents and other materials containing confidential information about the Company or its clients, customers, suppliers or distributors. You must not disclose confidential information to a new employer or to others after ceasing to be an employee of the Company.

If there are any questions concerning confidential information or the treatment of what is believed to be Company's confidential information, please contact the Company's General Counsel or Human Resources. Additional resources around confidential information can be found in the Company's privacy and security policies.

H. Handling External Communications

Only those with the requisite authorization are permitted to communicate with the media and other outside parties on behalf of the Company. All media inquiries regarding DataBank and its operation must be referred to the Senior Vice President (SVP) of Marketing. Refer to Databank Information Security Policies and Standards Manual ("DB Infosec Manual") for further details.

If you receive an inquiry from any external source requesting a statement regarding DataBank's business, please maintain politeness and courtesy at all times. Then, direct the inquiry to the SVP of Marketing at marketing@ databank.com. If any employee happens to be approached by the media, by a trespasser or protestor, do not engage with them aside from providing them with the contact information for DataBank Marketing group. Employees should then notify their supervisor or security. Always presume you are being recorded, even if it is not immediately noticeable.

I. Protection and Proper Use of the Company's Assets

All DataBankers should protect the Company's assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Company's profitability. Any suspected incident of fraud or theft should be immediately reported to the Company's General Counsel, Human Resources or through the EthicsPoint Hotline. All of the Company's assets should be used only for legitimate business purposes, although incidental personal use may be permitted with the permission of your supervisor. The Company

has the ability, and reserves the right, to monitor all electronic and telephonic communication. You are encouraged to consult DataBank's Information Technology Acceptable Use & Privacy policy for further guidance.

J. Maintaining Accurate Books and Records

The Company's responsibilities to its investors require that all of the Company's books, records, accounts and financial statements, appropriately reflect the Company's transactions and conform to applicable legal requirements, the Company's system of internal controls and accounting principles generally accepted in the United States ("GAAP"). The Company relies on the accuracy and completeness of its business records to (i) make management decisions and (ii) analyze its operations.

The creation and maintenance of books and records that are honest, accurate, complete, timely documented and updated is vital for both our business's effective operation and DataBank's disclosure and financial accountability requirements. To fulfill the Company's responsibilities, DataBank employees are required to adhere to Company protocols to guarantee that business transactions are uniformly executed, documented, and reported in a manner that permits the Company to accurately compile and report its financial statements and other necessary information for running the business.

Any attempt to conceal, alter, tweak, or falsify data in DataBank's books and records is both illegal and unethical. Any breach of these principles will lead to disciplinary action, including termination and potential criminal prosecution. If you possess knowledge of or suspect any irregularities or issues regarding DataBank's accounting or records, it is your duty to report this information in accordance with the procedures outlined under section F of the Code. Moreover, all books and records should be retained for the necessary amount of time in alignment with company policies documented in the DB Infosec Manual.

All DataBankers with supervisory responsibility must implement and enforce the consistent execution of DataBank internal controls over financial reporting in their respective areas, when applicable. These controls have been designed to mitigate the risks of material financial misstatements and fraud.

K. Retention of Business Records

DataBank acknowledges its responsibility to preserve information relating to pending litigation, audits and investigations. Failure on the part of employees to take measures to safeguard and preserve company records in accordance with DataBank's records handling and retention schedules, as indicated within the DB Infosec Manual, this Code, and/or specific instructions provided related to litigation can result in possible civil and criminal sanctions against the Company, as well as possible disciplinary action against responsible individuals (up to and including termination of employment). All DataBankers must comply at all times with all laws, rules and regulations relating to records preservation, any records retention policies and any document or record preservation notices. Records must be maintained for the duration of the assigned retention periods.

Records are information created or received on any storage medium and kept because they represent the position, transactions, or business of the Company. Non-records encompass materials such as copies for convenience, materials publicly available, items related to non-business activities, and preliminary papers, drafts, and versions deemed non-critical. Refer to the DB Infosec Manual for further guidance on what constitutes non-records.

It is DataBank's policy to manage the Records Management Program adhering to the following principles:

- Comply with legal and regulatory requirements at the state, federal, regional, and international level, including those linked to litigation, governmental investigation, and auditing.
- Retain records for the durations specified in DataBank's retention schedules.
- Adequately dispose of records in alignment with the policies in the DB Infosec Manual, except where legal holds exist.
- Eliminate records as soon as they are no longer required, as per guidance provided in the DB Infosec Manual.

L. Fraud, Anti-Bribery, and Anti-Corruption

DataBank is committed to fostering a culture based on ethical behavior and values. To this end, fraudulent activities are forbidden. Fraudulent activities include theft, the misappropriation or misuse of assets for personal benefit; bribery and corruption; false accounting and/or making fraudulent statements with a view to personal gain or gain for another: for example, falsely claiming overtime, travel and subsistence, sick leave, or special leave (with or without pay); externally perpetrated fraud against an organization. The Company's board of directors (Directors) is tasked with identifying fraud risk and ensuring compliance with this policy to prevent fraud. Everyone within the Company is responsible for detecting potentially fraudulent activities and reporting them to the General Counsel, Human Resources or the EthicsPoint Hotline (see Section O. Employment Practices and Human Rights).

i. Foreign Corrupt Practices Act (FCPA)

The Company conducts its business in certain international locations. This can present the unique challenge of trying to observe local business customs while still complying with applicable U.S. and other laws prohibiting corruption.

It is the Company's policy to comply with all applicable anti-bribery and anti-corruption laws. The FCPA, the U.K. Bribery Act 2010, and other anti-corruption laws prohibit any payment or offer of payment to a "foreign official" for the purpose of influencing that official to assist in obtaining or retaining business for a company. The Company has established a robust FCPA policy, to ensure that all employees of the Company, its agents, and its affiliates are aware of the FCPA requirements and engage in ethical and legal practices. DataBank's full FCPA policy can be found in the DataBank Employee Handbook, available for internal use only.

M. Anti-Boycott

Occasionally, overseas governments may instigate boycotts or economic sanctions against other countries. However, U.S. anti-boycott legislation typically forbids individuals or companies from taking part in or cooperating with international boycotts that are not endorsed by the United States. Furthermore, U.S. individuals and companies are obligated to inform the government of any requests for them to cooperate or participate in a foreign boycott. If you receive any request or demand possibly subject to anti-boycott laws, please contact DataBank's General Counsel or a member of the Compliance team for guidance.

N. Political Contributions and Interactions with Government

The Company's funds or assets may not be contributed, directly or indirectly, to any political party, committee or candidate, or the holder of any federal, state or local government office within the United

States. DataBankers shall not be directed, pressured or coerced in any manner by an officer or any individual acting in a managerial or supervisory capacity to contribute to any political party or committee or to any candidate for or the holder of any government office.

Any DataBanker, acting solely in their personal capacity, may participate in political activity and make political contributions at their own expense. Personal contributions, for which no reimbursement is sought, are not affected by this Code.

O. Employment Practices and Human Rights

i. Equal Employment Opportunity

The Company forbids discrimination against any person on the basis of race, religion, color, creed, sex, sexual orientation, gender, sexual/gender identity, age, disability, pregnancy, national origin, citizenship, military or veteran status, marital status, genetic characteristic or information, ancestry or any other characteristic prohibited by applicable law.

ii. Anti-Harassment and Non-Discrimination

The Company is committed to maintaining a workplace free from harassment, intimidation and hostility. The Company prohibits sexual, racial and other unlawful harassment in the workplace. The Company will not tolerate undue influence, offensive behavior, sexual harassment, intimidation, or other disrespectful conduct by one DataBanker toward another or by any DataBanker toward a customer, resident or supplier. For additional information on diversity, equity, and inclusion principles, please see our Workforce Excellence Statement.

iii. Anti-Human Trafficking, Forced Labor, and Child Labor

The Company is committed to a work environment that is free from human trafficking and slavery. The Company will not and does not tolerate or condone human trafficking in any part of its organization or business relationships. Trafficking in persons is an international crime involving the acquisition of a human being through the use of force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age, for the purpose of exploiting the individual, adult or child, for profit through forced labor, prostitution or both. It constitutes a violation of human rights in which the victims are deprived of their fundamental freedoms. This policy is intended to comply with the requirements of Federal Acquisition Regulation Subpart 22.17 and 52.222-50, to the extent applicable to the Company. To the extent, if any, this policy conflicts with applicable law, controlling law will be applied. DataBank's full Anti-Human Trafficking Policy can be found in the Employee Handbook, available for internal use only.

iv. Human Rights

The Company is committed to protecting human rights. Consistent with the United Nation's Universal Declaration of Human Rights, the Company understands human rights are fundamental rights that apply to all peoples regardless of nationality, ethnicity, race, age, gender or gender identity, religion, sexual orientation, political beliefs or disability. In upholding human rights, we prohibit harassment, bullying discrimination, use of child or forced labor, or trafficking in persons for any purpose. The Company supports human rights by treating DataBankers, shareholders and partners with respect and by providing fair employee policies and competitive compensation. Human rights are protected across all DataBankers and extended to investors, partners, customers, vendors, contractors, and suppliers. Any suspected violation of human rights can be reported anonymously to the Company's EthicsPoint Hotline using the contact information as provided in section R of this code.

Employees may also report suspected violations through established channels including their supervisors, General Counsel, or Human Resources.

P. Health and Safety

The health and safety of DataBankers and others on Company property are of critical concern to the Company. The Company intends to comply with all health and safety laws applicable to our business. To this end, Company must rely upon employees to ensure that work areas are kept safe and free of hazardous conditions. DataBankers are required to be conscientious about workplace safety, including proper operating methods, and recognize dangerous conditions or hazards. Our health and safety practices extend to our customers, partners, contractors, vendors, suppliers, and visitors. Any unsafe conditions, potential hazards, injury, accident, or serious illness occurring on Company property should be reported to the employee's supervisor and through Company Incident Reporting within 24 hours of the incident, regardless of the severity. Any suspicion of a concealed danger present on the Company's premises, or in a product, facility, piece of equipment, process or business practice for which the Company is responsible should be brought to the attention of management immediately.

Periodically, the Company may issue rules and guidelines governing workplace safety and health. All employees should familiarize themselves with these rules and guidelines, as strict compliance will be expected.

Firearms are prohibited in the Company's facilities and/or its owned or leased property to the fullest extent permitted by applicable law.

Additional health and safety considerations can be found in the Company EHS Policy.

Q. Environment and Sustainability

At DataBank we are committed to protecting the environment and reducing our consumption of resources. We have set a net zero goal by 2030 and developed EHS and Climate Policies, all of which we expect DataBankers as well as our customers, partners, vendors, and suppliers to support. DataBankers must comply with all regulatory and legal requirements pertaining to the environment. Further, DataBankers should support Company's efforts to minimize energy and other resource consumption by following Company procedures and standards and alerting management to any visible or otherwise perceived deviance from these procedures.

R. Reporting Violations (Whistleblower Policy)

i. Duty to Report

The Company requires all employees to observe high standards of business and personal ethics in the conduct of their duties and responsibilities. DataBank's employees must practice honesty and integrity in fulfilling their responsibilities and comply with all applicable laws and regulations. This Code covers a wide range of business practices and procedures, but it does not address every applicable law or respond to every ethical question or concern that may arise. Nonetheless, the general guidelines of this Code provide each DataBanker with the Company's expectations regarding business dealings. The Company understands that there may be some situations in which it is difficult to know right from wrong. In determining whether an action is appropriate, each DataBanker should answer the following questions to help evaluate specific situations:

1. Will my action comply with the intent and purpose of the Company's policies and practices?
2. Will I compromise myself or the reputation of the Company by this action if it becomes known to my supervisor, colleagues, shareholders or friends?
3. Is this action honest in every respect?
4. Could this action appear inappropriate to others, even if it is ethical?

If something you have seen, heard or been asked to do (or not do) seem illegal, unethical or improper, express your concerns so that the matter can be thoroughly investigated and addressed. Every DataBank employee has a direct responsibility to promptly report to the Company any real, attempted, or apparent violation of the law or this Code.

ii. Reporting Procedures

The CEO or President & CFO has the responsibility to escalate suspected or actual violations of this Code that could significantly impact the Company's reputation, legal standing, or ethical posture to the Board of Directors. DataBank has an open-door policy and encourages employees to share their questions, concerns, suggestions, or complaints with their supervisor. If you are not comfortable speaking with your supervisor or you are not satisfied with your supervisor's response, you are encouraged to speak with the VP of Human Resources (HR) or the Senior Director, HR. Alternatively, DataBank EthicsPoint Hotline provides the option for customers, vendors, and other stakeholders to file a report. Lastly, DataBank, in partnership with NAVEX Global, an independent company, allows employees, and other stakeholders, to confidentially report concerns 24/7 either online or via toll-free telephone.

Reporting Contacts	
Human Resources	HR@databank.com
EthicsPoint Hotline	• Online: www.databank.ethicspoint.com • Mobile Devices: www.databankmobile.ethicspoint.com • US Toll-Free: 844-979-4929 • UK Toll-Free: Dial 0-800-89-0011, then dial 844-979-4929

iii. Confidentiality

Violations or suspected violations may be submitted on a confidential basis by the complainant. Reports of violations or suspected violations will be kept confidential to the extent reasonably practicable, consistent with the need to conduct an adequate investigation. All submitted reports will be promptly investigated, and appropriate corrective action will be taken, if warranted.

iv. No Retaliation

The Company will not tolerate retaliation against any DataBanker for raising, in good faith, a possible violation of this Code or of a law, rule or regulation. Federal law prohibits retaliation for reporting a federal offense. Any DataBanker who participates in retaliatory conduct will be subject to disciplinary action up to and including termination of employment. Misusing this Code by knowingly or recklessly providing false information to the Company may also result in appropriate disciplinary action.

Every officer, manager and supervisor who receives a complaint or a report alleging or regarding an actual or potential violation of this Code or of a law, rule or regulation has, without exception, the responsibility to immediately communicate such complaint to Human Resources at the addresses above or report it through the EthicsPoint Hotline.

S. Waivers of or Changes to the Code of Business Conduct and Ethics

In the unusual event where it would be suitable to waive this Code, such an exemption for a DataBank employee who is not a senior executive must be authorized by the Chief Executive Officer (CEO) or a person to whom this responsibility is explicitly assigned in writing or in accordance with policies and procedures sanctioned in writing by the CEO. Any waiver of the Code for a member of the Company's board or executive officer must be approved by the Audit Committee or the full board. The majority of the members of the Audit Committee voting to approve the waiver must be impartial Directors, as defined by relevant law, concerning the matter leading to the necessity for a waiver. Any waiver of this Code approved for an executive officer will be revealed promptly as per the requirement of the law or listing standards.

T. Administration and Implementation

The Directors have overall responsibility for administering and interpreting this Code. The Company's General Counsel and Human Resources are responsible for the implementation of this Code.

U. Other Compliance Policies and Procedures

Each DataBanker acknowledges and is aware of certain other policies and procedures of the Company, or segments thereof, that may apply to such DataBanker, including, but not limited to, corporate governance guidelines.

All such policies are readily accessible from the Company's General Counsel and Human Resources and/or internal information technology portals available to all DataBankers. If any uncertainty or question arises upon review of any one or more such policies and procedures, do not hesitate to clarify with the Company's General Counsel or Human Resources.

V. Website Disclosure

This Code, as may be amended from time to time, shall be posted on the Company's website.

Approved: March 2025

