Bentley®

BENTLEY SYSTEMS, INCORPORATED AND ITS SUBSIDIARIES

CODE OF CONDUCT

Last reviewed August 2023

Bentley®

Table of Contents

CODE OF CONDUCT

1. Introduction.

The Board of Directors (the "Board") of Bentley Systems, Incorporated ("Bentley Systems") has appointed a management level Compliance Committee to assist the Board and its audit committee with implementing and monitoring this Code of Conduct (the "Code") and ensuring that this Code is clearly communicated to all of the employees, officers and directors of Bentley Systems and its subsidiaries (collectively referred to as the "Company"). The Company's employees, officers, and directors are each individually referred to herein as a "colleague" and collectively referred to herein as "colleagues". Members of the Company's extended workforce (temps, interns, graduate trainees) and others who may be contracted to perform work or services for Bentley are expected to follow the Code and are also, for the purposes of this Code, considered "colleagues" in respect to their work for Bentley.

The Code has been designed to enhance the ability of the Company to compete effectively by setting forth an appropriate standard of business conduct protecting the Company and its colleagues. The Code must be adhered to by every colleague. The Code touches on many types of activities and behavior which, if engaged in by colleagues, could expose the Company and its colleagues to liability. Violations or breaches of the Code may lead to disciplinary action including dismissal from employment. It is the responsibility of every colleague to adhere to the Code and to report suspected violations of the Code as described herein.

The Code is not intended to reduce or limit the other obligations that colleagues may have to the Company, including but not limited to those obligations set forth in the Company's Employee Handbook (as defined below) and Insider Trading Policy, which include policies on business conduct which supplement and are in addition to this Code. The term "Employee Handbook" shall refer to a colleague's local Employee Handbook (as modified from time to time), or, if a local Employee Handbook does not exist, shall refer to the corporate Employee Handbook (as modified from time to time). In the case of the Company's non-employee directors, compliance with this Code is subject to provisions of the Company's organizational documents and any stockholder's agreement with the Company.

PLEASE CAREFULLY READ THE PROVISIONS OF THE CODE SET FORTH BELOW. ALL COLLEAGUES ARE, BY REASON OF THEIR CONTINUING EMPLOYMENT BY THE COMPANY, DEEMED BOUND BY THE CODE, AS IT MAY BE MODIFIED FROM TIME TO TIME BY THE COMPANY. AFTER YOU HAVE READ THE CODE, PLEASE CLICK THE "ACKNOWLEDGED" BUTTON AT THE CONCLUSION OF THE CODE BELOW TO ACKNOWLEDGE THAT YOU HAVE READ THE CODE, THAT YOU ARE BOUND BY THE CODE, THAT YOU UNDERSTAND ITS PROVISIONS AND THAT THE VIOLATION OF ANY PROVISION OF THE CODE MAY BE GROUNDS FOR DISCIPLINARY ACTION, INCLUDING TERMINATION OF EMPLOYMENT. THE COMPANY RESERVES THE RIGHT TO MAKE CHANGES TO THE CODE. COLLEAGUES ARE REQUIRED TO REVIEW AND ACKNOWLEDGE THE CODE ANNUALLY AS PART OF THE COMPANY'S ANNUAL COMPLIANCE TRAINING PROCEDURES.

2. Administration and Disciplinary Action.

2.1 Policies and Procedures.

The Company's policies and procedures have been developed over time and are periodically revised as required or otherwise deemed necessary or appropriate. Each colleague must understand and follow them. The Code serves as a guide for colleagues when faced with legal or ethical questions. The Code is not all-inclusive, however, and we do not expect the Code to answer every possible question that may come up in the course of conducting business. The Company expects colleagues to use their own reasonable judgment at all times to follow the high ethical standards to which the Company is committed. If you are concerned about an ethical situation or are not sure whether specific conduct meets the Company's standards of conduct, you are responsible for asking your supervisors or managers and, where appropriate, the Company's Legal Department, any question that you feel is necessary to understand the Company's expectations of you. There is no conflict or inconsistency between good business and good ethics.

2.2 Compliance Committee.

The Compliance Committee will be comprised of five officers of the Company appointed by the Board from time to time, one of which will be appointed the Chairman of the Compliance Committee. The list of members of the Compliance Committee shall be maintained separately by the Company's Legal Department.

The primary role of the Compliance Committee is to assist the Board with implementing and monitoring compliance with the Code and to update and modify the Code from time to time in response to changes in the Company's legal and business environment. The Compliance Committee is also responsible for assuring the education of colleagues with regard to the Code. The Compliance Committee must be kept fully informed of potential Code violations and issues, and whenever necessary, or at the request of the Board, including its Audit Committee, or the Chief Executive Officer or Chief Legal Officer, the Compliance Committee may be specifically directed to coordinate or otherwise manage investigations of reports made under the Code. The Compliance Committee will maintain a log of all records relating to any reports made under the Code, tracking their receipt, investigation and resolution and the response to the person making the report. The Company shall retain copies of the reports and the Compliance Committee's log for a period of ten years, unless notified by the Chief Legal Officer of an extended retention period.

2.3 Procedure For Reporting Violations of the Code and Accounting Concerns.

You have an obligation to alert the Company to any situation in which the Code is being violated or you believe is about to be violated. You should make a report if you are concerned that a Company practice or operation or a colleague's action violates a law, rule or regulation, Company policy, or accounting or auditing principal or practice. You should also report any alleged retaliation against colleagues who make good faith reports. You are protected from retaliation for good faith and whistleblower reporting regardless of the outcome of the investigation. You are encouraged to talk to supervisors and

managers about actual or suspected illegal or unethical behavior and when in doubt about the best course of action in a particular situation. Any supervisor or manager who receives a report of a violation covered by this Section must report it immediately to the Compliance Committee.

In addition to contacting your supervisors and managers, you may communicate any violations, suspected violations or concerns in any of the following ways:

- Send a message via a dedicated, externally managed web site available at the URL https://www.openboard.info/BSY. This reporting site is available 24 hours a day, seven days a week. As an employee, your anonymity is assured by the third-party web site service, unless you choose to state your identity.

- Send a letter to the Compliance Committee at the following address:

  Bentley Systems,
  Incorporated Compliance
  Committee
  685 Stockton Drive
  Exton, PA
  19341 USA

Bentley is committed to the timely assessment of every report and, where appropriate, conducting an investigation of the matter by the appropriate department(s) (e.g., Legal, Compliance HR, etc.). Reports and investigations are reported to the Compliance Committee and the Board of Directors.

In addition, the reporting procedures above may be used for complaints and concerns regarding accounting, internal accounting controls or auditing matters, as more specifically described in Annex A hereto. Upon receiving any such report involving the Company's senior management team or having an actual or potential misreporting or loss to the Company that could have a material effect on the Company's reputation or financial statements the Compliance Committee must forward such report to the Audit Committee. If you are concerned that your report is not being addressed in an appropriate and timely manner, or you otherwise wish to contact the Board directly, you may contact the Audit committee by sending a letter addressed to the Chair of the Audit Committee at the Company's address in Exton as set forth above. Upon receiving any report covered by this paragraph, the Audit Committee must promptly determine whether to commence an investigation thereof.

Unless necessary to conduct an adequate investigation or compelled by judicial or other legal process, the Company will protect the identity of any colleague who reports potential misconduct and who asks that their identity remain confidential. The Company will also use reasonable efforts to protect the identity of the person about or against whom an allegation is brought, unless and until it is determined that a violation has occurred. Any person involved in any investigation in any capacity of possible misconduct must not discuss or disclose any information to anyone outside of the investigation unless required by law or when seeking his or her own legal advice, and is expected to cooperate fully in any investigation. To the extent practicable, the Company will acknowledge receipt of reports.

Notwithstanding any confidentiality requirements in this Code, and notwithstanding any other confidentiality or non-disclosure agreement (whether in writing or otherwise, including without limitation as part of an employment agreement, separation agreement or similar employment or compensation arrangement) applicable to current or former employees, this Code does not restrict any current or former employee from communicating, cooperating or filing a complaint with a U.S. federal, state or local governmental or law enforcement branch, agency or entity (collectively, a "Governmental Entity") with respect to possible violations of any U.S. federal, state or local law or regulation, or otherwise making disclosures to any Governmental Entity, in each case, that are protected under the whistleblower provisions of any such law or regulation, provided that (i) in each case such communications and disclosures are consistent with applicable law and (ii) the information subject to such disclosure was not obtained by the current or former employee through a communication that was subject to the attorney-client privilege, unless such disclosure of that information would otherwise be permitted by an attorney pursuant to 17 CFR 205.3(d)(2), applicable state attorney conduct rules, or otherwise. Any agreement in conflict with the foregoing is hereby deemed amended by the Company to be consistent with the foregoing.

Any other interested party may report to the Company any violations or suspected violations of this Code, the policies referenced herein or any other applicable legal or regulatory requirement or that concerns any accounting, internal accounting controls or auditing matters. Any such report must be accompanied by the name of the person submitting the report.

2.4 Disciplinary Action.

Any colleague who violates this Code or the Company's ethical standards is subject to disciplinary action which can include reprimand, probation, suspension, demotion or immediate termination. All colleagues should also be aware that certain actions and omissions prohibited by the Company's policies may violate the laws of the U.S. and/or other jurisdictions in which we operate and could lead to civil liability and damages, regulatory sanction and/or criminal prosecution.

2.5 Protection from Retaliation.

A colleague who reports incidents that he or she in good faith believes to be violations of this Code, or who provides information or otherwise assists the Company or any Governmental Entity in an investigation under this Code, will not be subject to reprisal or retaliation for such participation. Retaliation is a serious violation of this Code and should be reported immediately. The report and investigation of allegations of retaliation will follow the procedures set forth in this Code. Any person found to have retaliated against a colleague for reporting or for participating in an investigation of allegations in good faith will be subject to appropriate disciplinary action.

Any use of these reporting procedures in bad faith or in a false or frivolous manner, however, will be considered a violation of this Code.

2.6 Waivers of the Code.

Any waiver of any provision of this Code for executive officers or directors of the Company must be approved by the Board or a committee of the Board and will be

promptly disclosed if and as required by applicable securities law and/or stock exchange rules

3. Business Conduct.

3.1 Good Judgment and High Ethical Standards.

Colleagues must conduct all business affairs with honesty, fairness and integrity. These qualities are evidenced by truthfulness and the absence of deception or fraud. Any failure by a colleague to conduct oneself with integrity and honesty is a violation of the Code and, in circumstances where the colleague gains a personal benefit from the violation, may constitute actionable fraud.

At all times, you must exercise care in conversation, written communications and the preparation of documents for the Company. In any investigation or litigation involving the Company, the opposing party will have the right to examine the Company's records (electronic and hard copy) and every word colleagues write or speak may be inspected. It is therefore important that common sense and good judgment be used in written communications, the drafting of documents (including e-mail) and in conversations. All communications should stick to the facts. Conjecture, exaggeration and overly colorful language should be avoided. A good guide is not to say or put on paper anything you would not be willing to repeat before, or explain to, a judge or jury.

3.2 Conflicts of Interest and Acceptance of Gifts.

3.2.1. Avoid Conflict of Interests. Colleagues should avoid situations which involve or may involve a conflict between your personal interests and the interests of the Company. Exceptions to this policy may only be made after full disclosure to, and review and approval of specific or general categories by (i) the Compliance Committee (in the case of employees) or (ii) the Board or a committee thereof (in the case of executive officers or directors). A conflict of interest occurs if your activities or personal interests may influence or appear to influence the objective decision required by performance of your responsibilities for the Company. As in all other facets of their duties, colleagues dealing with user organizations, suppliers, contractors, competitors or any person doing or seeking to do business with the Company are to act in the best interests of the Company to the exclusion of considerations of personal preference or advantage. You are required to make prompt and full disclosure in writing to your manager of a prospective situation which may involve a conflict of interest. Such situations include, for example:

- Ownership by a colleague or, to the colleague's knowledge, by a member of the colleague's family of a significant financial interest in any outside enterprise which does or seeks to do business with or is a competitor of the Company (ownership of less than 1% of a publicly-traded company will not be considered "significant" for this purpose).

- Serving as a director, officer, partner, consultant, or in a managerial position with, or employment in any capacity by, any outside enterprise which does or is seeking to do business with or is a competitor of the Company.

- Acting as a broker, finder, go-between or otherwise for the benefit of a third

party in transactions involving or potentially involving the Company or its interests.

- Taking part in a Company business decision that involves a company with which such person or such person's family members have a personal affiliation or a Company decision that involves hiring or supervising a family member.

- Any other arrangement, including family or other personal or financial relationships, which might dissuade the colleague from acting in the best interests of the Company.

3.2.2. Receipt of Gifts and Payments by the Company. Colleagues shall not offer, give, solicit or accept inappropriate gifts, benefits, favors or entertainment from any person or business organization that does or seeks to do business with, or is a competitor of, the Company. In furtherance of this policy:

- Colleagues must not offer or receive anything of value in relation to obtaining business benefit or awarding contracts which is outside approved remuneration arrangements.

- It is never permissible to accept a gift in cash or cash equivalents (e.g. stocks or other marketable securities) of any amount.

- In a colleague's dealings on behalf of the Company, he or she may not realize any profit apart from his or her compensation from the Company.

- See also Section 3.4 "Bribery, Kickbacks, Gratuities and Other Improper Payments or Services."

3.2.3. Corporate Assets.

Theft, carelessness and waste have a direct impact on the Company's profitability. Colleagues have a duty to safeguard Company assets and ensure their efficient use. The Company acknowledges that an immaterial amount of certain corporate assets (such as expendable items like stationary and other office supplies) may be utilized by colleagues for personal use, but excessive personal use of any corporate assets (including expendable items and non-expendable items such as physical facilities and information systems) is prohibited. The misuse or removal without proper authorization from the Company's offices of any of its property is prohibited. Company assets include tangible property, intellectual property such as patents, trademarks, business and proprietary information such as new products, salary information and any unpublished financial data and reports. Unauthorized use or distribution of this information is a violation of this Code. This policy also applies to any property designed, created, obtained, purchased, leased, or copied by the Company for its own use including without limitation, files, reference manuals, user guides, reports, forms, policies, computer programs and software, data processing systems and databases.

See the section of this Code entitled "Information and Computer Systems Policy" for further detail about use of software and personal use of telephones, e-mail and the Internet.

3.3 Competition and Fair Dealing.

We seek to outperform our competitors fairly and honestly. We seek competitive advantages through superior performance, never through unethical or illegal business practices. Stealing proprietary information, possessing trade secret information that was obtained without the owner's consent, or inducing such disclosures by past or present employees of other companies, is prohibited. Colleagues should endeavor to respect the rights of and deal fairly with the Company's customers, suppliers, competitors, and employees. No colleague should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other intentional unfair-dealing practice.

3.4 Anti-Corruption, Anti-Bribery, and Improper Payments or Services.

We have zero tolerance for bribery and corruption. Bentley observes all applicable anti-corruption and anti-bribery laws and regulations of the countries in which we do business. It is a violation of the Code for any colleague to offer or receive a bribe, kickback, gratuity or other improper payment or service in order to achieve a desired business result. Providing or receiving a bribe, kickback, gratuity or other improper payment or service should for this purpose be assumed to constitute an unfair practice and may be illegal. Colleagues who become aware of a request for, or the offering of, any bribe, kickback, gratuity or other improper payment or service, whether or not they are personally involved, are required to report such occurrence to the Compliance Committee. Colleagues are regularly required to complete anti-bribery and anti-corruption training to better understand what constitutes bribery and corruption, how to avoid high-risk activity, and tactics to prevent bribery and corruption.

Colleagues are not permitted to offer anything of value to a government official in an effort to influence such official or to receive preferential treatment for the Company. Any questions arising regarding the application of this portion of the Code should be immediately directed to the Chief Legal Officer.

No colleague may extend or receive a bribe, kickback, gratuity or other improper payment or service from representatives of any company (for instance, but not limited to vendors or user organizations), to influence the placement of business. This prohibition extends to the provision or receipt of free or compensating services for which the recipient would normally incur an expense. Provision or receipt of free services may create an actual conflict of interest and may seem inappropriate, even if completely innocent in nature. Offers of such a bribe, kickback, gratuity or other improper payment or service must be reported to the Compliance Committee immediately.

In the normal course of conducting routine business activities, many colleagues entertain (or are entertained by) user organizations, vendors and others outside of the Company. Any entertainment must be reasonable and not excessive. It is impossible to prescribe a hard and fast rule for defining "reasonable" entertainment. A good way to measure the reasonableness of the entertainment is to think how you would explain the entertainment to a regulator or investigator at a later date. If the entertainment in question is of such magnitude that it could be perceived as a factor in a business decision, such entertainment is probably unreasonable and should be avoided. Examples of

entertainment that would appear to be reasonable would include a single sporting event or dinner. Examples of entertainment that would appear to be unreasonable could include free travel to resort areas for other than business purposes, the provision of season tickets for a professional sports team, and the like.

This is an area where a great deal of caution must be exercised by all colleagues. It is a violation of the Code for any colleague to approve an invoice without including in the related Purchase Request an accurate description of the services or goods being purchased by the Company. Colleagues must consult with the Chief Legal Officer any time they have a question under this Code about the propriety of any payment or benefit they are contemplating to incur or have been offered.

3.5 Accuracy of Records and Disclosure.

It is the Company's policy to make full, fair, accurate, timely and understandable disclosures in compliance with applicable laws and regulations in all reports and documents that the Company files with, or submits to, the U.S. Securities and Exchange Commission, U.S. state agencies, and in all other public communications made by the Company.

The integrity, reliability and accuracy in all material respects of the Company's books, records and financial statements are fundamental to the Company's continued and future business success. In addition, as a company whose stock is publicly-traded, the Company is subject to a number of laws and regulations that govern our business records, including U.S. securities laws. The Company must record its financial activities in compliance with all applicable laws and accounting practices and provide current, complete and accurate information to any and all government agencies. No colleague may cause the Company to enter into a transaction with the intent to document or record it in a deceptive or unlawful manner. In addition, no colleague may create any false or artificial documentation or book entry for any transaction entered into by the Company. Similarly, colleagues who have responsibility for accounting and financial reporting matters have a responsibility to accurately record all funds, assets and transactions on the Company's books and records.

3.6 Compliance with Laws, Rules and Regulations.

Obeying the law, both in letter and in spirit, is one of the foundations on which the Company's ethical standards are built. In conducting the business of the Company, colleagues must respect and obey the laws of the jurisdictions in which we operate. Although not all colleagues are expected to know the details of these laws, it is important to know enough about the applicable local, state and national laws to determine when to seek advice from the Company's Legal Department or other appropriate personnel. If a law conflicts with any Company policy or this Code, you must comply with the law. There are serious consequences for failing to follow any applicable laws, rules and regulations, including termination of service and potential criminal and civil penalties.

Please refer to our Insider Trading Policy for the Company's policies with respect to improper trading of securities.

3.7 **Tax Evasion**.

The Company takes a zero-tolerance approach to all forms of tax evasion. The Company is committed to acting with integrity in all business dealings and relationships and will uphold all applicable laws relevant to countering tax evasion. Colleagues and others who provide services to or act on behalf of the Company must not take any action that causes the Company to commit a tax evasion offense or that facilitates a tax evasion offense by a third party.

Tax evasion is not the same as tax avoidance or tax planning. Tax evasion involves deliberate and dishonest conduct. Tax avoidance is not illegal and involves taking steps within the law to minimize tax payable or maximize tax relief. This Code cannot address the complexities of all applicable tax laws and regulations, and questions concerning the application of this policy should be referred to the Legal Department.

3.7.1. Facilitation of Tax Evasion. Facilitation of tax evasion means knowingly being concerned in, or taking steps with a view to, the fraudulent evasion of tax by another person. Facilitation of tax evasion can subject the Company and individuals involved to criminal penalties.

It is prohibited for any colleague to:

- engage in any form of facilitating tax evasion under the applicable laws of any country;
- aid, abet, counsel, or procure the commission of a tax evasion offence by another person;
- fail to promptly report any request or demand from any third party to facilitate the fraudulent evasion of tax by another person;
- engage in any other activity that might lead to a breach of this policy; or
- threaten or retaliate against another individual who has refused to commit a tax evasion offence or who has raised concerns under this policy.

3.7.2. Prevention of Tax Evasion. There is no exhaustive list of tax evasion opportunities. Colleagues and others working on behalf of the Company should adopt a common- sense approach to detecting potential tax evasion opportunities. Unusual payment methods or conduct of third parties can be indicative that a transaction may not be as it seems.

3.7.3. Reporting Concerns. The prevention, detection, and reporting of tax evasion are the responsibility of all colleagues and those providing services to or working on behalf of the Company. If you become aware of any fraudulent evasion of tax by another person, or you are asked to assist another person in their fraudulent evasion of tax, or if you believe or suspect that any fraudulent evasion of tax has occurred or may occur, you must notify the Company in accordance with Section 2.3 as soon as possible.

3.8 Antitrust.

The Company is committed to vigorous competition in the marketplace. Conduct or behavior aimed at limiting competition is inconsistent with this commitment and may violate state and federal antitrust laws. Such violations may result in serious consequences. For instance, conduct violating the antitrust laws may result in severe criminal penalties. In addition, antitrust violations may result in costly private lawsuits and civil damages. This Code requires full and complete compliance with all antitrust laws. The following sections outline some of the major aspects of the antitrust laws. This brief overview cannot address the complexities of all of the antitrust regulations. Colleagues should refer any questions regarding the application of these policies to the Chief Legal Officer.

3.8.1. **Price Fixing**. It is a criminal violation of the antitrust laws to enter into any agreement or understanding, no matter how informal, with a competitor concerning the price of a product or service. This prohibition applies to any agreement or understanding to increase, decrease, or stabilize prices and any agreements or understandings concerning the terms or conditions of a sale. The simple exchange of price-related information between competitors, such as costs, profit margins or commission structures can be used to infer an agreement or understanding to fix prices. Colleagues are prohibited from any agreements, understandings or discussions with competitors related to prices or terms of business.

3.8.2. **Agreements to Divide Markets/Customers**. It is a criminal violation of the antitrust laws for competitors to agree to allocate markets, business opportunities, territories, or customers among themselves. The Company may not agree with a competitor to refuse to bid for particular types of business or otherwise refrain from competing for certain user organizations or classes of user organizations. Such market allocation agreements or understandings are prosecuted vigorously by the government. Involvement in such activities exposes the Company to significant potential liability and may also expose individuals involved to serious personal liability. Colleagues are prohibited from any agreements, understandings or discussions with competitors of the type described above.

3.8.3. **Group Boycotts/Refusals to Deal**. Group boycotts, or concerted refusals to deal, may be illegal. Accordingly, while the Company has the right to select those companies and individuals with whom it will and will not conduct business, the Company may not agree with any of its competitors, user organizations or others not to do business with another person or entity. No colleague may participate in discussions with a competitor, user organization or other entity concerning changing the status of any of the Company's business relationships with another party. Similarly, while the Company can refuse to do business with an entity on the basis of a poor history of business relations; the Company may not advise other entities not to deal with such entity, nor may the Company refuse to do business with an individual or entity at the request of another entity.

3.8.4. **Monopolization and Market Power**. It is illegal for a company to control prices within a particular market or to exclude others from that market through that company's size and market power. Market power alone, however, is not illegal. An illegal monopoly is one that is obtained or maintained through an abuse of power. This Code

prohibits the use of competitive tactics that could be construed as being designed to exclude or destroy competition in any market. Thus, it is contrary to this Code to say or do anything designed to harm a competitor except through the Company's superior product, marketing, positioning, pricing, terms, and service. Questions about the legality of any particular competitive tactic should be directed to the Chief Legal Officer.

3.8.5. **Tying or Reciprocity**. "Tying" and "Reciprocity" are the mirror images of each other. Tying is the refusal to sell one product or service unless the user organization buys another product or service. Reciprocity is the refusal of a purchaser to buy a product or service unless the seller agrees to buy some other product from the purchaser. Such agreements may be illegal if they allow a company to use its power in one market to obtain an unfair advantage in another market. Any tying or reciprocal agreement raises potential antitrust concerns and must be reviewed in advance by the Chief Legal Officer.

3.8.6. **Other Agreements Among Competitors**. Not all cooperative activity between competitors automatically violates the antitrust laws. Some cooperative activity may increase or be consistent with competition. Because of the risk that cooperative activity may be illegal, however, colleagues must consult with the Chief Legal Officer prior to taking any steps to participate in a cooperative arrangement with competitors.

3.8.7. **Trade and Professional Associations**. Trade associations and professional groups provide legitimate opportunities for valuable business, social and educational activities for their members. These activities are legal and permissible under the various antitrust statutes. However, trade association meetings of necessity bring together competitors and thus present opportunities for activities that may not be permissible. Discussions relating to issues and information of a sensitive, competitive nature must be avoided. Any mention to competitors of cost levels, marketing strategies, user organizations, territories and any other issues with an impact on competition between the Company and others is prohibited. If in connection with a trade or professional association meeting, any discussion begins that deals with competitively sensitive issues, representatives of the Company in attendance should attempt to stop the discussion immediately. If the discussion continues, the Company's representatives must leave the meeting immediately. Prior to leaving, an effort should be made to have an entry made into the formal minutes (if any) of the meeting detailing the reason that the Company's representatives chose to leave. A detailed written report on the incident should be prepared and forwarded to the Chief Legal Officer.

3.8.8. **Agreements Regarding Salary Levels or Hiring Practices**. The Company may not agree with other employers to limit pay increases. Nor may the Company agree with another employer to refrain from hiring each other's employees or in any other way not to compete with respect to hiring (except in some limited circumstances with commercial justification, such as subcontract relationships). Discussions or arrangements with other employers (other than through responses to industry or regional surveys conducted by recognized independent organizations) regarding salary levels or hiring practices, from which agreements concerning compensation and hiring practices might be inferred, are prohibited.

3.8.9. **Collection of Competitive Information**. The Company is entitled to

collect information concerning the competitive practices of its competitors. Such market information enables the Company to offer services and products in the marketplace that are competitively priced and better than those of the competition. However, an exchange of information between competitors may indicate the existence of an antitrust conspiracy. Accordingly, no colleague should obtain competitive information (even if the information is publicly available) directly from a competitor (other than through a publicly available website, and without subterfuge as to the colleague's identity) for purpose of limiting competition. Similarly, no colleague should provide competitive information to a competitor. It is permissible to obtain competitive information from third parties such as user organizations. It is also acceptable to obtain the information from public sources such as filings with state and federal agencies. Whenever a colleague obtains competitive information, the source of the information should be documented.

3.9 Political Contributions.

Colleagues may not use corporate funds to contribute to a political party, committee, organization or to any candidate in connection with a campaign, except as set forth below in this Section. This policy does not preclude (a) colleagues from making personal contributions to campaigns of their own choice, (b) the operation of a political action committee (such as the Bentley Federal Political Action Committee) under applicable laws, (c) Company contributions, where lawful, to support or oppose public referenda or similar ballot issues, or (d) the use of corporate funds for political contributions, where lawful, if reviewed and approved by the Chief Legal Officer. Questions regarding campaign contributions should be directed to the Legal Department.

3.10 Money Laundering and Antiterrorism.

The Company is committed to complying fully with all applicable anti-money laundering and anti-terrorism laws in the countries where we do business. Money laundering generally describes the process of concealing the nature and origin of funds connected with criminal activity, such as terrorism, trafficking, or bribery.

The Company does business only with reputable customers and partners involved in legitimate business activities, with funds derived from legitimate sources. Involvement in money laundering can expose the Company and individuals to severe sanctions, including criminal prosecution.

Colleagues must not knowingly engage in transactions that facilitate money laundering or result in unlawful diversion of funds. Colleagues are required to comply with all Company policies, standards, and other procedures designed to detect and deter suspicious forms of payment, customers, or transactions that could involve money laundering, including meeting accounting, record-keeping, financial reporting, and due diligence obligations as appropriate.

Compliance with anti-money laundering and antiterrorism laws and regulations requires colleagues to be alert to suspicious or unusual activities that may arise in the course of conducting business. Questions about the application of this policy should be referred to the Chief Legal Officer.

If you suspect that any money laundering activity has occurred or may occur, you

must notify the Company in accordance with Section 2.3 as soon as possible.

3.11 Economic Sanctions and Export Controls.

It is the policy of the Company to comply fully with the economic sanctions and export laws and regulations of the United States government and of any other applicable jurisdiction or country. Applicable sanctions and export controls may restrict the license of the Company's products, and the provision of technical information about, and maintenance and support services (including, installation, training, customization, repair, and providing updates and upgrades) for those products, to certain countries, companies, organizations, and individuals, or to parties involved in prohibited end uses.

Economic sanctions may prohibit the Company from doing business with certain designated countries and territories, organizations and individuals. and Export controls generally apply to cross-border oral, written, electronic, or visual disclosure, shipment, transfer, or transmission of technology (information, technical data, or assistance) or software. Disclosure of U.S. origin technology or source code to non-U.S. persons may also be subject to sanctions and export controls, even if the disclosure happens in the United States.

Failure to observe economic sanctions and export control laws and regulations can result in civil penalties and heavy fines, as well as criminal charges against the Company and other colleagues.

All colleagues must understand and comply with applicable sanctions and export control laws and regulations, as well as the related Company policies, guidelines, and procedures that apply to your area of responsibility. Any questions should be directed to the contacts identified in applicable Company guidelines, or to the Chief Legal Officer.

3.11 Workplace Policies and Procedures.

Colleagues are responsible for understanding and following the Company's Workplace Policies set forth on the Company's Human Resources website. Any potential violations of the Workplace Policies shall be reported to the colleague's manager.

3.12 Use of False Identity at Trade Shows and Online Events.

Colleagues are prohibited from using a deceptive name or identity to enter trade shows or online events. For example, colleagues may not enter a trade show or online event by use of another person's name or by stating that he or she works for a company other than Bentley Systems or its affiliates. This section, however, does not prohibit colleagues from entering online events anonymously by use of a non-descriptive user ID such as a personal e-mail address.

4. Confidentiality.

4.1 Company Confidential Information.

In the course of his or her participation in the work of the Company, colleagues may obtain or have access to non-public information that might be of use to competitors, or harmful to the Company or the other source of such information, if disclosed. Such

information may have been or may be provided in written or electronic form or orally. All such information, from whatever source obtained and regardless of the Company's connection to the information, is referred to herein as "confidential information."

The Company is strongly committed to protecting confidential information, whether generated within the Company or obtained from some other source. The Company is also strongly committed to avoiding the misuse, or the appearance of misuse, of such information, whether in connection with the trading of securities or otherwise. Colleagues must maintain the confidentiality of confidential information, except when disclosure is either expressly authorized by the Company or required by law.

Non-public information, or otherwise information that has been disclosed in violation of confidentiality obligations, relating to the operations and results of operations of the Company (past, present and future), its colleagues, business or user organizations or any information designated by the Company as "confidential" shall not be disclosed or used by any colleague except as expressly authorized by the Company.

Information relating to the competitive plans of the Company including, without limitation, products under development, marketing plans or promotions, user organization lists and any other information relating to the Company's marketing plans, or relating to the Company's information technology, including, without limitation, technical data, and computer software, is to be kept confidential. No such information shall be disclosed to any person outside the Company except as expressly authorized by the Company.

All colleagues are required to take the appropriate precautions to safeguard confidential and proprietary information of the Company that is under their control.

4.2 Third Party Confidential Information.

Colleagues may, in connection with their prior employment by another company or otherwise, possess confidential or proprietary information that belongs to third parties and that has not been disclosed to the Company. Such third-party confidential information should not be applied in connection with any work for the Company or disclosed to other colleagues.

4.3 Media Communications.

Only those colleagues who are expressly authorized by the Chief Communications Officer, a member of the Executive Cabinet or a Corporate Marketing designee may speak or write to the media or the public in the name of the Company. Any such communications must also be considered in light of the relevant section of our Corporate Communications & Regulation FD Policy.

In any Internet communication using Company systems, colleagues must at all times adhere to all Company policies, and refrain from expressing personal opinions or unauthorized political, religious or other advocacy. Colleagues also must refrain from unauthorized endorsement or appearance of endorsement of any non-Company commercial product or service. These requirements apply even when a colleague believes that he or she has not been identified as a colleague or agent.

Unless authorized by management, colleagues are prohibited from using

Company computer systems to discuss the Company or matters related to the Company in chat rooms or discussion groups (other than those maintained by the Company), even if the colleague is not identified at that time as a Company representative or employee.

5. Workplace Conduct.

5.1 Non-Discrimination, Freedom of Association, and Equal Employment Opportunity.

The Company recognizes the freedom, rights and dignity to which each individual colleague and applicant for employment is entitled. The Company is committed to providing equal employment opportunities, and a work environment free of discrimination, for all of its colleagues and applicants. The Company supports freedom of association and the rights of colleagues to lawfully and peacefully associate, organize and bargain collectively.

Each colleague is encouraged to consult the Employee Handbook for a complete statement of the Company's applicable Non-Discrimination and Equal Employment Opportunity Policy.

The Company is committed to equal opportunity in employment. The Company promotes a workplace where equal employment opportunity is provided without regard to age, race, color, sex, religion, national origin, sexual orientation, disability, covered veteran status, or any other status protected by law. We expect all colleagues to support our commitment to equal employment opportunity for all.

5.2 Fair Labor Practices and Human Rights.

As an organization with a global workforce and handprint, The Company is committed to upholding internationally proclaimed human rights. As part of this commitment, the Company supports the International Labor Organization's (ILO) Declaration on Fundamental Principles and Rights at Work's eight conventions. These fundamental conventions uphold workers' rights to organize and collectively bargain; eliminate forced labor; bar child labor; and protect workers against discrimination. The Company promotes and protects fair labor practices including providing or exceeding the minimum wage wherever we do business.

5.3 Harassment.

The Company is committed to maintaining a work environment that is free of any form of employee harassment based on sex, race, color, religion, national origin, age, disability, marital status, sexual orientation, veteran status or any other unlawful basis. The Company will not tolerate sexual advances, actions, innuendo, or comments, racial or religious slurs or jokes, or any other comments or conduct that creates, encourages or permits an offensive or intimidating work environment whether intentionally or unintentionally. Each colleague is encouraged to refer to the Employee Handbook for a complete statement of the Company's applicable Harassment Policy.

5.4 Respect in the Workplace.

The Company is committed to a workplace in which colleagues are treated with dignity, respect, and professionalism. Inappropriate behavior in violation of this policy includes behavior directed against an individual colleague or a group of colleagues that undermines colleagues' right to dignity at work and an environment where they can do their best. Such inappropriate behavior, often called bullying, may include personal insults, abusive language, unjustified or constant criticism, harsh public criticism, assignment of impossible goals, or other behavior that deliberately demeans, undermines, humiliates, isolates, or intimidates. It is important to keep in mind that routine discipline, correction, or critique by a manager are generally not considered violations of this provision. Training on respect in the workplace, including courses on recognizing and reporting bullying and abusive conduct, have been required for all colleagues.

5.5 **Maintaining Health and Safety**.

The Company is committed to maintaining a healthy, safe, and productive workplace. We integrate sound health and safety practices into our operations and business and comply with applicable workplace safety regulations. Colleagues must comply with all safety rules and should report unsafe situations immediately.

5.6 **Violence**.

The Company is committed to providing colleagues with a safe workplace, free of violence and intimidation.

Any type of violent behavior including any threats, threatening language or any other acts of aggression or violence made against a colleague, client, visitor or anyone by anyone while on Company premises or business is absolutely prohibited. Threats of violence include throwing objects, menacing gestures, damaging property, stalking or verbal or physical abuse. Possession

of any weapons or dangerous materials on Company premises is absolutely prohibited.

Colleagues who witness or are the victims of violent behavior or threats of violence must report the information to their immediate manager and/or Human Resources immediately.

Colleagues who are aware of a potential risk of violence at the Company from an individual not related to the Company (such as an ex-spouse, partner, boyfriend or girlfriend) are encouraged
to report that information to their immediate manager or to Human Resources. Any colleague that has obtained a protective or restraining order that lists the Company's locations as protected areas must provide a copy of the order to the Director of Human Resources, the Chief Legal Officer, or the Compliance Committee.

5.7 **Substance Abuse**.

The Company is committed to providing a safe workplace and to establishing policies that promote and encourage high standards of colleague health and safety. It is impossible to maintain a safe, healthy working environment if any colleague allows the use of alcohol or drugs to interfere with the performance of his or her job. Colleagues are encouraged to refer to the Employee Handbook for a complete statement of the

Company's applicable Substance Abuse Policy.

6. Privacy and Personal Data.

The Company is committed to protecting and responsibly using the Personal Data of colleagues, customers, and other third parties. We follow local privacy and data protection laws that deal with Personal Data. We provide clear and accurate privacy notices when collecting and processing Personal Data. Colleagues are required to follow all Company polices, processes, and standard when involved in the collection, use, transfer, storage, or disposal of Personal Data.

The Company strives to abide by the following Privacy Principles:

- Personal Data must be collected and processed lawfully, fairly, and in a transparent manner;
- Personal Data should be purposefully collected and processed and used only for the purpose collected unless allowed otherwise by law;
- Personal Data should only be shared for limited and approved ways;
- We respect the rights of access, accuracy, correction, and deletion when required by law; and
- All employees are accountable to ensure that we practice these privacy principles when handling Personal Data in our job duties on behalf of the Company.

7. Information and Computer Systems Policy.

This Section 7 of the Code supplements the Company's Workplace Policies found on the Company's Human Resources website. The E-mail, Internet Usage, Software Piracy and Systems Monitoring subsections of the Company's Workplace Policies outline appropriate usage of the Company's information and computer systems. All colleagues are required to follow these policies.

7.1 Information and Computer Systems Covered by the Policy.

For the purposes of the Section, the "Systems" shall include, but are not limited to, the following:

- Electronic mail (e-mail) access and usage;
- E-mail addresses;
- Voice mail access and usage;
- Internet access and usage, including the World Wide Web and sites accessed using browser programs;
- Application and file servers;

- Computer networks;
- Instant messaging and collaboration services;
- Colleague workstations;
- Desktop, laptop or notebook computers, palm computers, personal data organizers or personal computers, irrespective of where used;
- Electronic media, including but not limited to floppy discs, compact discs ("CDs"), digital video discs ("DVDs") or magnetic tapes;
- Modems, printers and other peripheral equipment;
- Electronic files;
- Program applications;
- Phones, phone systems and phone numbers;
- Software, either owned or licensed by the Company;
- Files, records, data, messages and information on the System or its components;
- All other elements of the Company's computer facilities and networks; and
- Physical facilities which house the Company's systems.

7.2 Ownership of Systems.

All elements of the Company's Systems are owned or leased by, or licensed to, the Company. All Systems, including hardware and software, are the property of the Company.

Records, files, data, messages, information and electronic communications contained in these Systems are also the property of the Company. No colleague has any ownership interest or rights, to any degree, in any of the Company's Systems, or any of the records, files, data, messages, intellectual property or information contained in the Systems. Any Systems created by colleagues during the performance of their duties as colleagues are property of the Company.

7.3 Use of Company Systems.

7.3.1. Systems are for Company Business. The Company's Systems are provided to Colleagues at the Company's expense to assist Colleagues in carrying out the Company's business. The Company's Systems permit colleagues to perform their jobs, share files and communicate with each other internally and with selected outside individuals and companies that the Company, in its sole discretion, decides should be accessible for communication or connected to the System. The Company's Systems are to be accessed and/or used only for Company related business purposes, except that occasional personal use is permitted as long as such use does not interfere with or harm Company usage or activities. Use of Company Systems (including its networks or access

to the Internet) to engage in commercial activities for a colleague's own benefit, or for the benefit of any entity other than the Company, is expressly prohibited.

7.3.2. Prohibited Actions

It is prohibited for any colleague to:

- use any Company System to violate any Company policy, or any applicable law or regulation;
- damage or disable any Company System or System component;
- use any Company System to carry out any non-Company commercial business;
- without proper authorization, remove or destroy records, files, data, information, messages or communications on Company Systems, except pursuant to the Company's record retention policy;
- without proper authorization, access, review or use, or attempt to access, review or use, any records, files, data or other information in Company Systems;
- access, attempt to access, use or disseminate any password or security clearance of another colleague, or not assigned to colleague, except at the direction of the Information Technology Support Department ("ITS Department") in which case the owner of the password is responsible to change it immediately thereafter;
- breach or attempt to breach System security measures; or
- violate the copyright of the owner of copyrighted information (i.e. music sharing programs).

It is also prohibited for any colleague to access or use any Company System (including but not limited to e-mail or voice mail systems) to intentionally create, reference, send, transmit, distribute, print, publish, store or download any records, files, data, information, messages or communications which, in any manner:

- violates Company policies;
- harasses, threatens or abuses another individual or entity;
- references or contains unlawful, harmful, defamatory, offensive, discriminatory, vulgar, obscene, hateful, pornographic or otherwise objectionable material of any kind;
- could constitute or encourage conduct that would be considered a criminal offense, or otherwise a violation of any law, obligation or regulation having the force of law;
- advertises or promotes non-Company goods or services (other than immaterial personal items);

- contains non-authorized personal information in violation of applicable privacy policies;
- is the result of impersonating or purporting to be someone other than the colleague;
- allows non-authorized individuals or parties to access Company confidential or proprietary information;
- violates the patent, copyright or trademark rights of other parties;
- uses or discloses the confidential or proprietary information of other parties that the colleague does not have authorization to disclose;
- contains chain letters of any kind; or
- denigrates or is intended to denigrate the Company or its shareowners, directors, colleagues, agents, businesses, products or user organizations.

7.4 Company Access to and Monitoring of Systems.

7.4.1. Company Access and Monitoring. There are many reasons why the Company may need to access and/or monitor the Company's Systems, including but not limited to colleague e-mail, voice mail, Internet access or transmissions, computer files, the network or other Company property or Systems. Some of these reasons include the need to continue to conduct ongoing business, to access information or data when a colleague is unavailable; to respond to requests by outside auditors; to respond to or gather information relating to Company disputes or litigation; to maintain quality control; to conduct training activities; to monitor task or job performance or to investigate colleague conduct. The Company reserves the right, for any of the above-listed reasons or for no reason, and without notice, to access or monitor the Company's Systems or colleague usage or communications. Company Systems, their contents and System usage are subject to inspection, examination and/or monitoring by authorized Company representatives at any time, without notice to colleagues.

Additionally, the Company reserves the right, without notice to colleagues, to access, review, copy, modify or delete any information transmitted through or stored on its Systems or network, including e-mail communications, voice mail communications and word processing and data files. The Company further reserves the right to disclose any such information to any party (inside or outside the Company) that the Company, in its sole discretion, deems appropriate.

Any files, data, information or messages containing the personal information of a colleague as a result of the colleague making occasional use of a computer, telephone or other System component for personal purposes, including transmission of personal email or voice mail messages, will be treated no differently than other files. Accordingly, colleagues are not entitled to, and should have no expectation of, privacy or ownership with the use of the Systems, networks, e-mail, voice mail or other Systems, or with the transmission, receipt, or storage of information contained within them.

Colleagues should not use the Company's Systems, including but not limited to voice mail or e-mail, to send, receive or store any personal information that they wish to keep private.

Colleagues should be aware that System and System components may automatically record and store information relating to colleague usage of Company Systems.

7.4.2. **Deletion of Records or Files**. Colleagues should be aware that System hardware, software and programs record a variety of information and data, and that even when a colleague deletes or erases a record, file or electronic communication, in whole or in part, such deleted material may still be retrievable at a later time. Colleagues should consider the Company's computer facilities and network a shared-file system under which files sent, received or stored anywhere in the system will be available for review and use by any authorized representative of the Company. The same is true of records, files and electronic communications sent out of the office to third parties. Moreover, the recipient or reviewer of files often is able to retrieve "hidden" information and at least some of the material that the creator or sender of the file has "deleted."

7.5 Security and Passwords.

7.5.1. **System Security**. Security of the Systems is a key priority of the Company. Colleagues are prohibited from breaching, or attempting to breach, System security measures. If a colleague believes he or she has discovered a security problem on any of the Systems, he or she should notify his or her immediate manager, the Chief Information Security Officer, and the Senior Director of Product Security immediately. The colleague should not communicate or demonstrate the security problem to other colleagues or third parties, except in the authorized case of Security Champions and members of the Application Security team either identifying issues or reproducing issues reported by ethical hackers for the purpose of driving resolution of the issue.

7.5.2. **Passwords**. Colleagues are prohibited from using any password other than their own, except in cases where a system is used for testing and the testing protocol requires the use of a different username and password. Colleagues must protect against unauthorized access to files on which they are working (however, individual passwords do not prevent authorized Company representatives from accessing those files).

Colleagues may not disclose personal or system passwords to anyone other than Company representatives specifically authorized to receive them. Colleagues should use their best efforts to keep their password secure. If a colleague has reason to believe that someone else is aware of his or her password, he or she should immediately change it. If a colleague has reason to believe that someone else is aware of the password of a colleague or another individual, they should contact the ITS Department. Colleagues are responsible for any information transmitted through the network under their password. System logs exist on the servers that identify which colleague signs into which computer.

Colleagues are prohibited from using another individual's password without express written permission of the ITS Department, or from attempting to log on to the network as a system administrator, except on systems used for testing, when the testing protocol requires such action.

7.6 Confidential and Proprietary Information.

Unless special precautions are taken, communications and messages on the Internet, e-mail and voice mail systems pose a risk of interception by or distribution to non-authorized recipients.

7.6.1. Internet. Colleagues must assume that the Internet and similar services are not secure — that is, unless special encryption programs are utilized, messages may not be private and may be accessed by unauthorized persons. The ITS Department can assist if encryption is required. All colleagues must consult with their manager before sending or transmitting unencrypted confidential or proprietary Company information over the Internet.

7.6.2. E-mail, Voice Mail and Mobile Phones. Most e-mail messages are transmitted over the Internet. Additionally, most voice mail systems are susceptible to interception. The ITS Department can assist if encryption is required. All colleagues must consult with their manager before using voice mail or e-mail to send or transmit unencrypted confidential or proprietary Company information.

Additionally, it is important to recognize that voice mail and e-mail systems make it easy for someone to take a message or other information and preserve, copy or distribute that message to multiple parties, in some cases far beyond what the sender of the message intended. Accordingly, colleagues should carefully screen any e-mail or voice mail communication for content before transmission. Further, colleagues should use care in addressing e-mail or voice mail messages to make sure that messages are not inadvertently transmitted to an unauthorized user. In particular, colleagues should exercise care when using distribution lists to make sure that all addressees are appropriate recipients of the information. Individuals using lists are responsible for ensuring that the lists are current, and are accountable for the consequences if such lists are not current. The Company generally discourages the use of distribution lists by colleagues.

When discussing Company business on a mobile phone in a public place, colleagues should take reasonable precautions to ensure the privacy of such conversation.

7.6.3. Other Safeguards for Confidential or Proprietary Information. Confidential or proprietary information should never be transmitted or forwarded to outside individuals or companies not authorized to receive that information, or to other persons inside the Company who do not need to know that information.

Confidential or proprietary information should not be displayed on a computer screen when a computer is unattended.

Colleagues should not leave portable electronic media or backup tapes that contain confidential or proprietary information open to access by third persons. Such media should be kept locked in drawers or file cabinets.

If colleagues transmit any information to third parties using portable electronic media, colleagues should be sure that the item (floppy disk, CD, etc.) has not previously been used. Otherwise it may contain confidential information that the colleague did not intend to

transmit. That information may be retrievable even through an effort was made to “delete” it.

Colleagues should be aware that many electronic files contain “hidden” data such as author annotations, information concerning the creation and editing of the document, and recent changes to the document. Consult the ITS department before circulating any electronic file if you are concerned about the dissemination of such data.

7.7 **Software, Copyright and Use Restrictions**.

The Company licenses computer software from other companies. The Company may be precluded from copying or distributing such software, from installing it on certain machines or from disclosing it to third parties. It is prohibited for any colleague to take any action in violation of applicable license agreements.

Use of the Company’s Systems to unlawfully copy and/or transmit any software program, document or other information protected by the copyright laws is prohibited by U.S. federal law. Use of the Company’s Systems for this purpose may subject colleagues and the Company to civil and criminal penalties.

Colleagues must be aware of the danger of running software that is downloaded from the internet, or for which the authorship is unknown. Examples include programs that an internet site offers to install or that are attached to e-mail. Such programs often contain viruses or “spyware” and should never be installed or executed on any company system. However, there are valuable tools that are available without licensing fees or restrictions on the internet, for example for software development. Those may be downloaded by Colleagues if they assist in performing job responsibilities. Colleagues must use caution when installing or using such programs. If there is any question, obtain assistance and advance approval from the ITS Department.

7.8 **E-mail, Voice Mail and Internet Usage**.

It is not advisable to send “joking” or humorous messages. Intended sarcasm can be lost without facial expressions or voice intonations, and a later reading of the message can result in a distorted communication unintended by the original sender. Jokes or commentary concerning personal characteristics, lifestyle, gender, race, religion, national origin, disability or sexual orientation reflect bad judgment and are severely discouraged.

7.9 **Audits of the System**.

To ensure that colleagues comply with these policies, the Company may conduct periodic audits (either remotely or in person) of its Systems, including individual personal computers, portable electronic media and backup tapes. Additionally, companies that license software or other System components to the Company may have the right to audit Company and colleague usage.

Annex A

Accounting, internal accounting controls or auditing matters may include, without limitation:

1. fraud or deliberate error in the preparation, review or audit of financial statements of the Company;

2. fraud or deliberate error in the recording and maintaining of the Company's financial records;

3. deficiencies in, or non-compliance with, the Company's internal control over financial reporting;

4. misrepresentation or false statements regarding a matter contained in the Company's financial records, financial statements, audit reports or any filings made with the Securities and Exchange Commission (including periodic or current reports);

5. deviation from full and fair reporting of the Company's financial condition and results;

6. substantial variation in the Company's financial reporting methodology from prior practice or from generally accepted accounting principles without adequate public disclosure;

7. issues affecting the independence of the Company's independent registered public accounting firm;

8. falsification, concealment or inappropriate destruction of corporate or financial records; or

9. theft, fraud or other misappropriation of Company assets.