



## **ProAssurance Corporation Code of Ethics and Conduct**

### **1. Introduction**

*All employees and officers of ProAssurance Corporation and its subsidiaries (collectively referred to as “ProAssurance” and/or the “Company”) are responsible for conducting themselves in compliance with this Code of Ethics and Conduct (the “Code”) other Company policies, and applicable laws and regulations. In addition, all members of the Board of Directors of the Company, in connection with their duties as directors, are responsible for conducting themselves in compliance with applicable provisions of this Code, other Company policies, and applicable laws and regulations.*

*As used in this Code, the term “employee” means all employees and officers of the Company and members of the Board of Directors of the Company in connection with their duties as directors. The term “Corporate Compliance Officer” means one or more employees of the Company that are designated by the Company from time to time to act as the corporate compliance officer under the Code.*

#### **A. General Policy and Procedures**

The trusted name and good reputation of ProAssurance is the product of the conduct, dedication, integrity and competence of our employees. All insurance companies, including ours, depend on their reputations. The Company expects all employees to share its commitment to high ethical, legal and moral standards and to avoid any activities that could involve the Company or its employees in any unethical, improper or unlawful act. Careful study of this Code will provide employees with a clear understanding of the Company's expectations and their respective obligations. Compliance with this Code is mandatory, and all employees have a duty to familiarize themselves with the Code and the legal standards and policies applicable to their assigned duties, and to conduct themselves accordingly.

The Code is not intended, however, to be an exclusive set of guidelines or policies for governing the conduct of employees. The Company has adopted and may amend or adopt other corporate policies, procedures, personnel manuals or employee handbooks as deemed by management or the Board of Directors to be appropriate or necessary at any time. Moreover, no Code or set of policies can ever be totally comprehensive or serve as a substitute for the good judgment, common sense, and proper, ethical and legal conduct expected of all employees.

The Code can be found on the ProAssurance website ([www.proassurance.com](http://www.proassurance.com)), and a printed copy can be obtained from Human Resources. Employees may contact Human Resources for the identity of their current Corporate Compliance Officer. Any changes to this Code shall be disclosed to the public on ProAssurance's website within five business days after the change is made.

**B. Reporting of Violations.**

All employees of the Company are required to read, understand and fully comply with the Code and to disclose any relationships or activities that the Company needs to evaluate to ensure an employee's compliance with the Code. If an employee's circumstances change in a manner that might give rise to a violation of the Code, the employee must immediately discuss the matter with his or her manager and the Corporate Compliance Officer.

All employees shall promptly disclose any acts, circumstances, or transactions that are known to employee and that create the potential for a violation of the Code. The Audit Committee of the Board of Directors has adopted procedures for reporting violations of the Code, including mechanisms for reporting violations on a confidential and anonymous basis if desired. These procedures are set forth in the "Policies and Procedures for Collecting and Reviewing/ Complaints about Auditing and Accounting Matters/ Violations of the Code of Ethics/ Communications to Independent Directors" (the "Reporting Procedures"). A copy of the Reporting Procedures is available on the ProAssurance website or from Human Resources.

Employees are encouraged to use the Reporting Procedures to report violations of the Code. The Company will not tolerate retribution, retaliation or adverse personnel action of any kind against anyone for lawfully reporting a situation of potential noncompliance or breach of any Company policy, or providing to the Company or any law enforcement or other governmental agency any information or assistance relating to the commission or possible commission of any federal or state offense. Failure to report violations of the Code shall be grounds for disciplinary action.

**C. Disciplinary Action**

Any employee who fails to comply with the policies, standards and guidelines in this Code, or with the law and regulations applicable to the Company's businesses, is subject to disciplinary action which may include immediate dismissal, oral or written reprimand, probation or suspension. For example, disciplinary action may be taken against any of the following persons:

- Any employee who violates this Code or applicable laws and regulations or who directs others to do so.
- Any employee who deliberately withholds relevant information, or knowingly provides false information, or otherwise impedes an investigation concerning a violation of this Code or applicable laws and regulations.
- The violator's manager, to the extent that circumstances of a violation reflects the manager's disregard for this Code or applicable laws and regulations.
- Any employee who retaliates, directly or indirectly, against another employee for reporting a suspected violation of this Code or applicable laws and regulations, or assisting an investigation of a suspected violation.

Anyone with questions or doubts about the application of the Code or who is aware of or suspects a violation of the Code should follow the Reporting Procedures or consult with the Corporate Compliance Officer.

## **2. Employment Practices**

*The Company is committed to the principles of equal opportunity employment. All employees are entitled to be treated with dignity and respect.*

### **A. Equal Opportunity**

Every employee must comply with the spirit and intent of our equal opportunity employment policy. Employees must comply with and administer all Company programs and benefits according to their terms, without unlawful discrimination.

### **B. Harassment.**

The Company does not tolerate harassment of any of our employees, applicants, customers or business partners. Therefore, harassment against any employee based on a characteristic protected by applicable law is prohibited. This could include, but would not necessarily be limited to, harassment based on race, color, religion, gender, sexual orientation, gender identity or expression, national origin, age, genetic information, disability, or veteran status. The Company's No Harassment Policy contains detailed information on employees' and managers' responsibilities with respect to harassment, which includes a separate method of reporting and investigating instances of sexual harassment. Reports of harassment should be made as provided in the Code or in the No Harassment Policy.

## **3. Conflicts of Interest**

*Employees shall avoid employment or business activities, including personal investments, that interfere with their duties to the Company, divide their loyalty, or create or appear to create a conflict of interest.*

### **A. General**

It is not possible to provide a precise, comprehensive definition of a conflict of interest. However, one factor that is common to all conflict of interest situations is the possibility that a person's actions or decisions may be affected or may have the appearance of being affected because of an actual or potential divergence between the interests of the Company and some other interest, including that person's own personal interests. Conflicts of interest also arise when an employee or a member of his or her family receives improper personal benefits as a result of his or her position in the Company. Loans to, or guarantees of obligations of, such persons are of special concern. A particular activity or situation may be found to involve a conflict of interest even though it does not result in any financial loss to the Company and irrespective of the motivations of the person involved.

Employees must promptly report any situation or transaction involving an actual or potential conflict of interest to the Corporate Compliance Officer. The Company will determine whether the interest in question involves an actual or potential conflict based on the facts of each case.

### **B. Business or Investment Opportunities**

Employees owe a duty to the Company to advance its legitimate interests when the opportunity to do so arises. Employees are prohibited from (i) taking for themselves personally opportunities that are discovered through the use of Company information or position; (ii) using Company property, information, or position for personal gain; and (iii) competing with the Company.

No employee or member of the Board of Directors is permitted to purchase financial instruments (such as prepaid variable forward contracts, equity swaps, collars, and exchange funds) that are designed to hedge or offset any decrease in the market value of the Company's common stock that (i) have been granted to the employee or member of the Board of Directors as part of his or her compensation; or (ii) are otherwise held, directly or indirectly, by the employee or member of the Board of Directors.

**C. Employee Interest in Companies Transacting Business with the Company**

The Company selects providers of goods and services on the basis of merit, without favoritism. Accordingly, this Code requires that employees avoid any relationship or activity that may directly or indirectly impair their independence or judgment.

The Company recognizes that, from time to time, it may transact business with a company in which an employee or an employee's spouse or children ("Immediate Family") has an interest or is employed. The Company also recognizes, however, that such transactions could present conflicts of interest if the employee fails to disclose the relationship or participates in the approval process. Therefore, whenever the Company does business or considers doing business with a company in which an employee or member of an employee's Immediate Family is employed or has a material financial or other interest, the employee must: (i) disclose the interest to his or her supervisor if he or she is aware of the proposed business relationship, and (ii) refrain from participating in the approval process.

A conflict of interest may also arise where an employee or a member of his or her Immediate Family makes an investment in a company that does business or competes with the Company. If an employee or a member of his or her Immediate Family is considering such an investment, the employee must disclose the proposed investment in advance to his or her supervisor and seek approval for it. If approved, the employee must comply with any conditions of the approval and must not participate in any decision regarding the selection of, or purchase from, such entity.

This Section does not prohibit investment in any business where the percentage of ownership is insignificant. However, any such investment in publicly traded securities is prohibited and violates the Code if the employee invests while in possession of material, non-public information regarding such corporation that was derived from his or her position with the Company. This information would, for example, include knowledge about the Company's investments in, or relations or negotiations with, such corporation, if such information has not been generally released to the investing public.

**D. Outside Employment**

The Company recognizes and encourages the participation of employees in religious, charitable, educational and civic activities. Employees must exercise good judgment to avoid involvement in activities that would present a potential conflict of interest or interfere with responsibilities to, or the reputation of, the Company.

**E. Conflicts with Insureds**

If an employee or a member of the employee's Immediate Family has a dispute or claim adverse to any insured of the Company, the employee should notify his or her supervisor. The employee must not handle any matters pertaining to the insured or relevant to the claim.

## 4. Securities Transactions

*Employees are prohibited from trading the Company's securities while in possession of material non-public information.*

Generally, a person who during the course of his or her employment obtains confidential information about a company is considered an "insider." A person may be an "insider" for purposes of the law regardless of his or her position or title and regardless of whether he or she is included in the Company's list of "designated insiders." Insiders can be liable for fines, civil penalties and criminal penalties (including imprisonment) if they buy or sell securities on the basis of the material, non-public information. This includes purchasing securities to make a profit when information is favorable, as well as selling securities to avoid losses when information is unfavorable. An insider also can be liable for both civil and criminal penalties if he or she tells other persons the material, non-public information ("tipping") and those other persons buy or sell the securities on the basis of that information. The insider's employer may also be liable for such illegal trading by its employees. Therefore, if you know material, non-public information about the Company, you are prohibited from buying or selling the Company's securities or from tipping others until that information is publicly announced.

No employee of the Company, and no member of the Immediate Family or household of such person, shall engage in any transaction involving a purchase or sale of the Company's securities, during any time in which the person knows material, non-public information about the Company. Moreover, such persons should refrain from trading in the Company's securities, even after the material information has been released to the public, for a period sufficient to permit thorough public dissemination and evaluation of the information.

No employee shall disclose or communicate any material, non-public information about the Company to any other person when the information is used by such person to trade in the Company's securities.

The Company may establish Company-wide blackout periods in which no trading is permitted in Company securities. The undertaking of the Company to establish blackout periods does not, and will not, relieve the Company's employees of their individual responsibilities under this policy. The Company may elect to impose "regular blackout" periods for recurring events (such as the release of quarterly earnings) and "special blackout" periods for non-recurring developments that are material to the Company. Employees should treat the announcement of a "special blackout" period as material, non-public information with respect to the Company.

### A. **Material Information**

Material information about the Company is information that would be considered important to an investor in making an investment decision regarding the purchase or sale of the Company's securities. While it may sometimes be difficult under this standard to determine whether particular information is material, there are various categories of information that are particularly sensitive and, as a general rule, should always be considered material. Examples of such information include:

- Undisclosed financial results of the Company or any confidential revenue, expense, earnings or other financial projections for the Company;
- Any projected change in competitive conditions, regulatory or licensing matters or other industry conditions that could significantly affect the Company's revenues, expenses, earnings, financial position or future prospects;

- Any significant expansion or curtailment of operations, or any information regarding a significant change in the level of revenues, expenses or earnings of the Company, its subsidiaries or their operating divisions;
- Any proposal or negotiation for the acquisition of a substantial company, business or amount of assets, or the creation of a material joint venture or similar business enterprise in which the Company would be a participant;
- Any proposal or negotiation for the sale of a substantial subsidiary, division or business of the Company, or the termination of any substantial joint venture in which the Company is a participant;
- Any major change in the corporate structure or organization of the Company;
- Significant changes in Company management or key employees or the size of the Company's workforce;
- Any significant accounting adjustments, write up or write down of assets, or change in accounting methods;
- Any undisclosed significant litigation or governmental proceeding or investigation concerning the Company, any of its officers, directors or employees, or any significant client or operation of the Company, or any business occurrence or event that could give rise to material litigation or governmental proceedings or investigations;
- Material undisclosed cybersecurity incidents or breaches;
- Any proposed stock split or stock dividend or any proposal relating to the payment of cash dividends by the Company;
- The development of new products or lines of business; and
- Impending bankruptcy or financial liquidity problems.

The foregoing list is presented by way of example only and is not intended to be exhaustive. If an employee, officer or director has a question about whether any particular item would be considered "material information," the Corporate Compliance Officer should be consulted. The Corporate Compliance Officer will, after appropriate investigation, make all final determinations as to which information is material. **Moreover, whenever there is any doubt about whether particular information is material, employees must treat it as material.**

**B. Non-Public Information**

Information is "non-public" until it has been made available to investors generally (through a press release, SEC filings such as a Form 8K, etc.) and the market has had time to evaluate the information.

**C. Duty to Keep Material, Non-Public Information Confidential**

Material, non-public information relating to the Company is the property of the Company, and the unauthorized disclosure of such information is forbidden. All material, non-public information concerning the Company must be kept strictly confidential and should not be discussed with family, business or social acquaintances. Further, confidential information should not be discussed with other employees of the Company unless they have a right and need to know such information.

This policy regarding the use and disclosure of confidential information applies to inquiries about the Company and its subsidiaries that may be made by the financial press, market makers, brokers, investment analysts or others in the financial community. All such

communications on behalf of the Company or its subsidiaries must occur through an appropriately designated spokesperson under carefully controlled circumstances in accordance with the Company's Corporate Disclosure Policy. Unless an employee is expressly authorized to speak on the Company's behalf, he or she should decline comment upon receipt of a financial inquiry and refer the inquirer to the Company's designated spokesperson(s).

Individuals who violate this policy shall also be subject to disciplinary action by the Company, including termination of employment. If you have any doubt as to your responsibilities under this policy, seek clarification and guidance from the Corporate Compliance Officer or the Company's legal counsel before you act.

## **5. Confidentiality of Information**

*The Company's proprietary, confidential or non-public information must be handled properly in order to protect such information from unauthorized access, use and disclosure.*

### **A. Generally**

The protection of the Company's confidential and proprietary information is critically important to the Company's businesses, its ability to compete within the insurance industry and its compliance with applicable federal and state securities laws. By virtue of their service to, or employment by, the Company, employees may have access to the following types of confidential and proprietary information of the Company including, without limitation, information related to customers and prospective customers (referred to as "Confidential Information"):

- Insureds or other customers, actual or prospective, and the contents of their claims, underwriting and other files, including items covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or similar state privacy laws;
- Lists of insureds and or other customers, actual or prospective;
- Marketing, underwriting or financial plans or analyses which the Company does not distribute to the public;
- Claims practices or analyses which the Company does not distribute to the public;
- Information relating to pending or past litigation, claims, charges or demands in which the Company has been involved and which is not a matter of public record;
- All other strategic plans, analyses of operations, computer programs, personnel information and other proprietary information which the Company does not distribute to the public; and
- Personnel records and/or other information regarding current, former or potential employees.

All Confidential Information is the sole property of the Company. The Company and all employees have ethical and legal responsibilities to maintain and protect the confidentiality of all Confidential Information. Employees are required to secure from unauthorized access and public view all documents under such employee's control that contain Confidential Information. When such information is being discarded, steps must be taken to ensure proper destruction. Failure to adequately protect this information may have an adverse economic impact on the Company, and any misuse or disclosure of Confidential Information may result in violation of applicable state and federal laws, including securities laws and applicable insurance laws. Violations could expose the Company and/or the person involved to severe criminal or civil liability.

It is a violation of the Code for any employee, both during and after such person's service or employment with the Company, directly or indirectly, to use or disclose outside the Company, (including with a different employer or company) any Confidential Information, to any entity or person (including a person within the Company who does not have a need to know such Confidential Information) unless approved by the Company. Further, all employees must promptly deliver to the Company upon their resignation or termination of their relationship with the Company, or at any other time as the Company may so request, all materials and all copies of materials (including electronic copies stored on any digital media) containing or evidencing Confidential Information or any materials derived from or based upon such information.

**B. HIPAA**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") establishes regulations regarding electronic data interchange and the privacy of, access to, and security of protected health information ("PHI") for "Covered Entities" and "Business Associates" who assist a Covered Entity. Covered Entities include health plans, health care clearinghouses, and health care providers. Business Associates are those persons or entities who assist a Covered Entity in performing any function or activity regulated by HIPAA.

A Covered Entity must obtain satisfactory assurance that Business Associates will appropriately safeguard PHI. Satisfactory assurance is secured through the use of the Business Associate Agreement which, in part, addresses the permitted use and disclosure of PHI, responsibilities of the Business Associate, and responsibilities of the provider.

All employees are expected to familiarize themselves with the applicable requirements of HIPAA and a copy of any applicable Business Associate Agreements. Although the provision of liability insurance to a Covered Entity does not create a Business Associate relationship, the Company agrees with its insureds to protect PHI in a manner consistent with HIPAA.

**6. Compliance with Laws, Fair Dealing and Trade Practices**

*All employees are expected to comply fully with all federal and state laws and regulations applicable to the Company's businesses and with all applicable Company policies. Fraud, dishonesty or criminal conduct involving Company operations is prohibited.*

Employees occupy positions of trust and confidence. In discharging their responsibilities, each employee has a duty to serve the Company, in good faith, in a manner that he or she reasonably believes to be in the best interests of the Company and its stockholders and with such care as an ordinary prudent person in a like position would use under similar circumstances. Employees also have duties of candor, care and loyalty to the Company. Those duties may be violated if an employee engages in conduct such as theft of employee or Company property; misuse of computer, telephone, technology or mail resources; falsification of records or reports, including unauthorized signing another person's name, or any unauthorized alteration of a Company document; violation of expense reimbursement policy, the drug and alcohol policy or weapons prohibition policy; and violence or threats of violence.

The Company depends on its reputation for quality, service and integrity. The way the Company deals with its customers, goods and service providers, and competitors molds our reputation, builds long-term trust and ultimately determines our success. Employees should endeavor to deal fairly with the Company's customers, goods and service providers, competitors and their respective employees. Employees must never take unfair advantage of others through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or



any other unfair dealing practice.

The Company's businesses are subject to a wide range of federal and state laws, regulations and rules. Additionally, the Company's products and services are primarily contractual promises that may be subject to unfair trade or insurance practices laws and regulations. Employees shall not knowingly violate any law or regulation, including unfair trade or insurance practices laws. Highlighted below are some of the key compliance guidelines that must be followed.

- Employees may not engage in conduct or a sales practice that is intended to manipulate or take unfair advantage of a customer, provider or supplier, or misrepresent the Company or its products or services.
- Employees shall not misrepresent facts, contractual terms or Company policies to a customer, provider, supplier or regulator. If an employee does so inadvertently, he or she must correct the misrepresentation as soon as possible after consulting with a manager and Company's legal counsel or the Corporate Compliance Officer.
- Employees may not agree with competing companies to engage in any of the following illegal practices: fix prices; allocate or divide markets or customers; boycott or refuse to deal with competitors, customers, goods or service providers; or engage in any other behavior that unlawfully restrains competition.
- Employees may not discuss or exchange competitively sensitive confidential information (e.g., relating to price or markets) with representatives of competing companies, except with the prior approval of the Company's legal counsel.

Employees should consult with the Corporate Compliance Officer or the Company's legal counsel on any matter relating to actual or potential noncompliance with any law or regulation or any of the Company's contractual commitments.

## **7. Corporate Records and Reports**

*Illegal or improper record keeping and the unauthorized destruction of documents is prohibited.*

### **A. Record Keeping**

Accurate and complete record keeping is essential to the the Company's business and to enable us to comply with legal and regulatory requirements, to manage the affairs of the Company, and to provide the best possible service to its policyholders. The Company adheres to a strict policy of maintaining complete and accurate books and records. Employees must keep books, records and accounts that accurately and fairly reflect in reasonable detail all business transactions and disposition of assets. Off-balance sheet transactions, arrangements and obligations must not be executed, and unrecorded funds or assets must not be maintained unless permitted by applicable law or regulation.

### **B. Disclosures in Periodic Reports**

As a public company, ProAssurance is required to file various periodic reports with the Securities and Exchange Commission. In addition, the Company is required to file various reports with insurance departments in the states in which it does business. ProAssurance makes full, fair, accurate, timely and understandable disclosure in compliance with all applicable laws and regulations in all required periodic and other reports.

**C. Record Retention**

The Company has specific requirements for retaining various categories of records generated by the Company. In addition to these specific requirements, the Company must retain all records that have any bearing on threatened or pending litigation, investigations, or administrative proceedings.

Employees who are notified of the existence of a subpoena or have reason to believe that a government investigation is imminent or that legal proceedings may be instituted must retain all potentially relevant records in their possession, custody, or control, including papers, and electronically stored data, until they have been notified otherwise by the legal counsel for the Company. Also, managers should ensure that employees under their supervision retain all such records in their possession, custody, or control.

**D. Monitoring**

The Company reserves the right, but does not assume the obligation, to monitor or inspect information systems, including e-mail, Internet usage and personal computer files, and any other Company materials or property in order to prevent or detect improper record keeping or use of property or resources and to investigate possible violations of law, this Code or other Company policies.

**8. Use of the Company's Funds or Other Resources**

*The Company's funds, assets, services of the Company's personnel and other resources of the Company are to be utilized only for the benefit of the Company.*

The Company's funds, assets, services of the Company's personnel and other resources (collectively, "Resources") are to be used only for the benefit of the Company and for such other lawful and ethical uses as may be approved by the Company consistent with this Code. Company Resources may not be used for any unlawful purpose.

An employee who has access to Company funds must follow the Company's procedures for recording, handling and protecting money. Where an employee's position requires spending of Company funds or incurring any personal expenses to be later reimbursed by the Company, he or she must exercise good judgment on the Company's behalf and to ensure that good value is received for expenditures. Company funds should only be used for Company purposes and must not be used for personal benefit.

**A. Personal Use of the Company Funds or other Resources**

No employee shall use, or authorize any other person or entity to use, Company Resources for any purpose which is not for the benefit of the Company or otherwise permitted under Company policy consistent with this Code. Misappropriation of any Company Resources is theft and, in addition to subjecting a person to possible criminal and civil penalties, may result in immediate dismissal or other disciplinary action.

**B. Payments and Gifts to Governmental Officials**

Employees should not make or authorize any payment or gift for the purpose of inducing or influencing any governmental body or official to improperly grant special consideration to or forego any claim against the Company. No Company Resources may be used to make payments or gifts to any governmental body or official unless for a lawful purpose with the consent of the Corporate Compliance Officer.

**C. Payment and Gifts to Others**

Employees should avoid all circumstances in which a gift or entertainment could present or create the appearance of a conflict of interest or improper, unethical or illegal conduct. To avoid such circumstances, employees may give incidental gifts and entertainment to others on behalf of the Company, only if they are consistent with accepted business practice, are of sufficiently limited value, and in a form that will not be illegal and that will not create the appearance of a conflict or impropriety. No gift or entertainment is permitted if it violates any applicable laws or ethical standards. If there is any question in a specific situation, approval should be sought from the Corporate Compliance Officer. In all cases involving gifts or entertainment of substantial value, approval of the Corporate Compliance Officer must be sought in advance.

## **9. Receipt of Gifts, Loans, Favors, or Other Gratuities and Remuneration**

*Employees should not accept entertainment, gifts or favors that could influence, or appear to influence, business decisions in favor of any person or organization with which the Company has or is likely to have business dealings.*

In order to avoid the appearance of impropriety, no employee may solicit or accept from any outside concern that does, or is seeking to do, business with or competes with the Company any gift, favor, entertainment or other remuneration which goes beyond common courtesies generally associated with accepted business practices. No cash gifts of any amount are ever acceptable. If any gift, entertainment, favors or other enticement either obligates the Company to do business with the donor, or would cause embarrassment to the Company if publicly disclosed, the gift should be rejected or declined.

This Section shall not prohibit employees or members of their family from obtaining loans, goods or services made or provided in the ordinary course of business on the same terms as are generally available to the public from businesses and financial institutions that have relationships with the Company.

## **10. Political Contributions**

*The Company's funds, assets, services of the Company's personnel and other resources of the Company may not be used for illegal political contributions or in the illegal support of a political candidate for any office.*

There are three basic tenets of the Company's policy with respect to political contributions:

First, the Company unequivocally forbids the illegal use of Company Resources for the support of political parties or political candidates for any office (Federal, State or local) in the United States or any foreign country.

Second, the Company forbids pressure, direct or implied, that infringes upon the right of employees to decide whether, to whom, and in what amount they will make a political contribution or render services to individual candidates or political committees where permitted by applicable laws. Employees are free to endorse, advocate, contribute to, or otherwise support any political party, candidate or cause they may choose.

Third, any permitted political contributions of Company Resources must be approved by the Corporate Compliance Officer.

## 11. Technology Resources and Information Security

- A. *The purpose of the Company's technology resources, including telephone voice mail, e-mail, computer and related information and communication system, and electronically stored and transmitted data is to promote the effective performance of the Company business, and their use by employees must not violate this Code.*

The technology resources are maintained by the Company for Company business use.

Company information on Company technology resources and other systems is the sole and exclusive property of the Company and is subject to the confidentiality provisions under this Code. The Company reserves the right, but does not assume the obligation, to review an employee's use of the Company's technology resources and Internet usage. **Employees should understand that they have no privacy with respect to any personal information created, stored or communicated on or through the Company's technology resources.**

The Company does not allow any employee to make, utilize or give to other employees or third parties, any software used on the Company's computers unless authorized under the Company's license agreements. Employees are not permitted to duplicate software other than for back-up purposes without the permission of the Information Systems Department.

The Company's Technology Resources Policy is available through Human Resources and contains detailed information for employees regarding their use of the Company's technology resources and Internet usage.

- B. *All employees are expected to promptly report internally any indication of an actual or potential breach of any technology system or protected data.*

The Company maintains an Information Security Program, consisting of various specific policies, checklists, procedures and protocols, to ensure compliance with data privacy and breach reporting requirements and to secure the Company's technology resources and data in a responsible manner. Any employee who becomes aware that the Company's technology systems, files, or databases have been, or may have been, compromised by a phishing attack, ransomware, a lost or stolen device, a lost or stolen file, hacking or other method must promptly report that information to the Company's Chief Information Security Officer or other appropriate officer of the company.

## 12. Application/Waivers

*Employees of the Company, whether regular or temporary, full or part time, are subject to this Code. The Company will waive application of the policies set forth in this Code only where circumstances warrant granting a waiver.*

Waivers of the Code for directors and executive officers may be made only by the Company's Board of Directors as a whole or its Audit Committee or Nominating/Corporate Governance Committee and must be promptly disclosed as required by law or regulation. Any waiver of this Code for directors, executive officers, (including without limitation, the chief executive officer, the chief financial officer, the chief accounting officer, the corporate controller, or persons performing similar functions) shall be disclosed to the public within four business days after the waiver is granted by providing disclosure on the ProAssurance website, distributing a press release, or filing a current report on Form 8-K with the SEC. Any waiver for other employees must be in writing and may be granted only by the Chief Executive Officer or his designee in accordance with such procedures as may be established by the Audit Committee or the Nominating/Corporate Governance Committee.