Instructions: Have employee sign and date and then place in personnel file.

PRIVACY POLICY AND SAFEGUARDING AGREEMENT

The nature of our business is such that the Company has confidential and proprietary information relating to its business policies, practices, methods of operations, and customer lists. In addition, we deal with confidential and proprietary information received from our customers. Each employee should understand the importance of making sure this information is protected from disclosure to competitors, suppliers, vendors, and all other persons.

Every employee has a legal and ethical obligation to take all steps reasonably necessary in order to keep the Company's and clients' affairs confidential. This obligation continues even after an employee leaves the Company. Information obtained by the Company and its employees should be treated at all times with the utmost confidentiality and discretion and should not be disclosed to anyone other than Company employees and others having a need to know. For this purpose, all Company information and client information should be considered confidential unless, beyond any doubt, the information is widely known and its disclosure would not be detrimental to the client.

Conversations in public

Have conversations about Company and client matters only with those who have a need to know, and take care to avoid such conversations where those who do not need to know may overhear. Conversations about such information in public places, such as elevators, restaurants, and airplanes should be avoided, and confidential matters should not be discussed with spouses, other relatives, or friends.

Client documents and materials

Do not leave Company and client documents or materials where they can be seen by any unauthorized person, such as in unattended conference rooms, on your desk, near the fax machine, on copy machines, in the mail room, or any other public locations. Do not discard documents containing confidential information without first shredding the documents. Do not stay logged in to your computer without having a password-protected screen saver in operation.

Support Personnel and Vendors

Care should be taken to ensure that persons who are providing support to the Company (such as computerized data services, copy services, and experts) and Vendors receive only information which they have a need to know and the Business Office will inform them of the nature of the confidentiality and the measures taken to protect confidentiality. Support Personnel and Vendors must sign this Policy and Agreement before any customer information is shared with them.

Safekeeping of financial information

All financial information shall be kept confidential and locked in file cabinets each evening. Employees are not to take any financial information of the Company or its clients home to work on or otherwise remove it from the office unless there is specific business need to do so. Employees are not permitted to keep financial information, including credit applications, credit reports or contracts at their desks or on the fax machine for any purpose other than to collect the information and to immediately transfer/transmit the information to the financial institution or to management staff to be placed in locked storage. Customers and vendors should not be left

alone in your office unless all customer information is in locked storage. Financial information and other personal information should never be left unlocked at your desk for any reason or for any period of time, regardless of the reason or the fact that you are working on the information. You should never share financial information or other personal information with anyone else in the company unless it is necessary for the purpose of completing the business transaction. Such information should only be shared on a need-to-know basis. Customer information must be in a locked storage area at all times. You should check to make sure the storage area (whether it is a room, a cabinet or your desk drawer) is locked each time you access the storage area.

You should never share or divulge your password providing access to the computerized data for any reason under any circumstance. Your password should not be stored where others can access it but should be kept in locked storage or in another place where others cannot access it.

Downloading information on the Internet to our computer systems may provide outside access to our systems. Therefore, you must not download any information from the Internet to our computer system without written authorization from the Security Program Coordinator.

If you need to dispose of any documents containing customer information, you must shred the documents prior to deposing of them.

You should never transmit customer information over the Internet or by email, under any circumstances.

You should never store customers' non-public personal information or financial information on PDA's, portable computers or other electronic devices unless you have written authorization to do so by the Security Program Coordinator so that security issues can be addressed prior to placing such information at risk.

You must never provide customer information to any callers over the telephone even if they appear to be legitimate business inquiries. All communication of customer information should be through written secure means such as facsimile to a known service provider or vendor who has agreed to abide by our policy or through other secure (encrypted) transmission. If you receive a call from a person attempting to obtain customer information, you should immediately transfer them to the Security Program Coordinator who will report the incident to law enforcement officials if necessary.

You must never use or reproduce customer information, whether electronic or non-electronic, for your own personal use or the use of others for unless for approved business purposes.

If you cease to be employed at the company, you shall not access and may not review any customer information from the moment you are no longer employed.

Release of Confidential Information

In the event that an employee inadvertently releases confidential information, the employee should immediately inform his or her department manager so the appropriate action may be taken. Any release of information, whether or not intentional, may be grounds for disciplinary action, up to and including termination. By signing below, the employee also agrees that he/she will notify the department manager immediately if any anticipated threats or hazards to the security of customers' personal information are suspected or detected or if the employee is aware of unauthorized access or sharing of customer information.

CONFIDENTIALITY AGREEMENT

As an employee of the Company, the undersigned acknowledges that from time to time he or she will receive confidential and proprietary information concerning the business of the Company. The undersigned further acknowledges that such information, if shared directly or indirectly with third parties, could be detrimental to the Company because it would place the Company at a competitive disadvantage if disclosed, and that but for his or her employment at the Company he or she would not receive such information, as it is not available to the public.

Accordingly, the undersigned agrees that he or she, except as necessary to conduct business of the Company, shall not disclose, copy, communicate, or divulge to, or use the direct or indirect benefit of any person, firm, association, or company other than the Company, any material provided by the Company, including but not limited to business methods, business policies, procedures, techniques, research, or development projects or results, trade secrets, or other knowledge or process of or developed by the Company or any other confidential information relating to our dealing with the business operations or activities of the Company made known to the undersigned or learned or acquired by the undersigned while an employee of the Company.

When the undersigned leaves the employ of the Company, he or she agrees to return all of the Company's documents and property in his or her possession, including but not limited to manuals, drawings, notebooks, reports, customer lists, pricing lists, and/or prospect lists.

Confidential information or material of the Company includes any information or material: (a) generated, collected, or utilized by the Company in its operations relating to the actual or anticipated business or research and development of the Company or (b) suggested by or resulting from any task assigned to me or work performed by me for or on the behalf of the Company and that has not been made available generally to the public.

In addition to confidential information about the Company, the undersigned acknowledges that he or she will also receive confidential information about clients and customers of the Company. The undersigned agrees that all provisions of this agreement and the attached Privacy Statement applicable to confidential information belonging to the Company will also apply to information received from and/or about clients and customers. The undersigned agrees to comply with this agreement and the attached Privacy Statement and the Company's Information Security Program, or any amendments to these documents that may be made from time to time. I also agree to complete the required security training. I agree that I will not access or view any customer information that is not necessary to the performance of my job duties.

The undersigned acknowledges that violation of any part of this agreement is grounds for immediate termination.

_____ _____

Signature - Date