

Corporate Governance - Confidentiality of Information

The following sets forth minimum standards for the safeguarding of confidential or proprietary information by employees of Rodman & Renshaw Capital Group, Inc. (the "Company"). To the extent that any other internal policy of the Company or a Company subsidiary, business group, or office sets forth more stringent standards or requirements, such policy will control.

Confidential and Proprietary Information

In the course of your employment with the Company, you may create, receive, know of or gain access to information that is confidential and/or proprietary. Confidential and proprietary information may be in a physical form (on paper, in an e-mail, on a diskette, videotape, etc.) or may be knowledge acquired through conversations to which you are a party or that you overhear. Proprietary information may consist of any system, information, or process that could give the Company an advantage over its competitors.

Confidential information includes non-public information that you are expected to safeguard from disclosure to the public. All proprietary information is confidential information. Therefore, proprietary and confidential information will be collectively referred to in this Policy as "confidential information."

Examples of confidential information include, but are not limited to:

- Information about the Company's operations, results, earnings projections, strategies, clients or client relationships, proprietary products or employee records.
- Information about the Company's or a client's merger or acquisition transactions, securities positions, pending orders or plans to raise capital (whether through registered offering or offerings exempt from registration), or any other information that could be deemed material to the Company or one of its clients.

Employee Obligations Regarding Confidential Information

As a general rule, you should presume that any information you receive about the Company or its customers is confidential and, therefore, should be protected from disclosure. You have an obligation to safeguard confidential information, whether generated internally or acquired from other sources, and to use it only in the performance of your employment responsibilities. In particular:

- You may not personally profit from confidential information. You may not use confidential information to trade securities for your own (or related) accounts or to advise relatives, friends or other persons with respect to trading securities. For additional guidance on this issue, please refer to the Company's Policy on Insider Trading set forth in the Written Supervisory Procedures Manual, a copy of which may be obtained from the Company's compliance department or the Company's General Counsel.
- During and after your employment by the Company, you may not disclose confidential information to anyone outside the Company. You may not use (or permit anyone else to use) such information, except as required by your employment responsibilities at the Company.
- Upon termination of your employment, you must return to the Company all physical (including electronic) copies of confidential information as well as all other material

embodied in any physical or electronic form that is based on or derived from such information, without retaining any copies.

- You may not bring to the Company confidential information of any former employer or use such information to aid the business of the Company without the prior written consent of your former employer.
- You may not seek to obtain confidential information that may be in the possession of other persons or business units of the Company that you do not need to know to do your job.
- You may not share confidential information with other employees except on a strict need to know basis.

Basic Practices to Protect Confidentiality

Confidential information may be communicated only to those persons who need to know it for a legitimate business purpose. Confidential information relating to third parties is often governed by a confidentiality or non-disclosure agreement which may have terms more rigorous than those set forth below. Always confirm whether an applicable confidentiality or non-disclosure agreement exists and comply with its requirements. If you have any questions, seek the guidance of the Company's General Counsel. Confidential information may be communicated to other employees of the Company or to the Company's outside lawyers and other consultants only if:

- The recipient has a legitimate need for and is authorized to receive the information in connection with his or her employment responsibilities; and,
- No identifiable harm can reasonably be expected to result from communication of the information to the recipient.

Information should not be communicated if it would give rise to a conflict between the interests of the recipient and those of the Company or its clients, or if it is reasonably foreseeable that the recipient would misuse the information. Confidential information concerning a transaction may be shared with other participants in the transaction only to the extent necessary to effectuate the transaction and only insofar as is consistent with your obligation to serve the client's interests.

The following practices should be followed to help prevent the misuse of confidential information.

- Avoid discussing or even speculating about confidential matters in places where you may be overheard by people who do not have a valid need to know such information.
- Avoid discussing confidential information on cellular phones, and take great care when discussing such information on speaker phones. Do not discuss confidential information with relatives or social acquaintances.
- Always put confidential documents away when not in use and, based upon the sensitivity of the material, keep such documents in a locked desk or cabinet. Do not leave documents containing confidential information where they may be seen by persons who do not have a need to know the content of the documents.
- Avoid unnecessary copying of confidential documents.
- Do not use trash or recycling bins to dispose of confidential documents. If available, use shredders prior to disposal.
- Never distribute internal-use-only documents outside the Company.

- When necessary, use codewords to conceal clients' identities or information regarding clients' proposed business or transactions.
- Do not give your computer IDs and passwords to any other person. Password protect computers and log off when they are not in use.
- Be aware that the Internet and other external electronic mail carriers are not secure environments for the transmission of confidential information.
- If you notice unfamiliar or unauthorized people in your department, do not hesitate to notify Security.
- Be aware that your conduct, particularly deviations from your normal activities (e.g., a research analyst does not return phone calls, or a market maker stops making a market) can signal to others that you have confidential information.
- Know and abide by all applicable policies relating to firewalls and other information barriers.
- Comply with the specific terms of any confidentiality agreements of which you are aware.
- When employees join or leave the Company or transfer from one part of the Company to another, take precautions to protect against disclosure or misuse of confidential information that they may possess.
- Refer requests for information on the Company and third party securities from the financial community, such as securities analysts, brokers or investors, to the Company's Investor Relations contact.
- Refer requests for information on the Company and third party securities from the media or press to the Company's Chief Executive Officer or President.
- Refer requests for information from the Securities Exchange Commission or other regulators to the Company's General Counsel.

Seeking Advice/Reporting Disclosures of Confidential Information

If you believe that you or others have received confidential information inappropriately, inform your general counsel or compliance officer immediately to avoid any potential problems. If you are uncertain as to whether information is confidential, treat it as such and ask for guidance from your general counsel or compliance officer. Similarly, contact the Company's General Counsel, or compliance officer immediately if you believe that you have provided confidential information to somebody who does not have a valid need to know it.