EXHIBIT 3: POLICIES AND PROCEDURES TO PREVENT THE MISUSE OF MATERIAL NON-PUBLIC INFORMATION

HR Ratings treats all information it receives from an issuer, or member of the issuer's business group, or their accountants, attorneys, or other agents as “Material Non Public Information” or “Confidential information”.[1] HR Ratings signs confidentiality agreements with all its clients, employees, and vendors (with access to this type of information), to ensure a confidential treatment off the information received.

The Head Compliance Officer is responsible for following up on the signing of these agreements and for overseeing ongoing compliance. The confidential information that clients provide to the company cannot be used for any purpose other than the credit quality analysis for the client and the offering in question. Likewise, client information will be sent solely to the person or persons the client has designed as responsible for communication with HR Ratings and must be marked confidential.

In order to further protect private, non-public material information received from issuers in hard copy are delivered in a sealed folder with the name of the recipient person or area marked, also marked with a stamp indicating the confidentiality of its contents. Likewise, nformation received by e-mail is marked confidential and directed only to the persons authorized for this purpose.

As further described below, preventive and protective measures for files of all confidential information pertaining to each client will be treated according to the regulations established by the company in the Internal Control Manual, Code of Conduct, and the General Operating Plan. Paper and hard copy information will be scanned and stored in protected files shared on the Company's analysis network and/or in the internal electronic system for the control and follow-up of Company affairs, as well as the information received by e-mail.

Only the Senior Analyst, the Lead Analyst and the support analysts designated will have access to a specific client’s file in order to complete their respective tasks, in accordance with the procedure established in the Company’s Operations Manual, through the internal electronic system and the shared files on the Agency’s internal server for the control and follow-up of affairs.

Access to Client files that are stored on the internal electronic system for the control and follow-up of Company affairs will be via codes provided to the persons authorized to this effect. The access codes for the internal electronic system are provided and held by the Chief Operating Officer. Such codes provided to the analysts are individual, nontransferable, and confidential; therefore, will not, under any circumstance, be shared.

[1] Information is not considered confidential when it was widely known to HR Ratings at the time of its publication, or was public knowledge at the time of its revelation, or becomes public knowledge upon publication (due to an action not imputable to HR Ratings), or is approved in writing by the client for public disclosure, or whose disclosure is required by government agency or authority.

Likewise, the Company has a system of restricted access to files containing information shared on the internal network, allowing employees to access only those files and folders for which they are authorized, therefore no employee will access information that is not related to the matters in which they are involved.

The Chief Operating Officer, with the support of the IT department, will replicate the permissions established for the Agency's internal electronic system to the shared files on the Agency's internal server.

The members of the Compliance and Risk Departments will have full access to the client files on the Agency's internal electronic control and monitoring system, and also to the information contained in the shared folders of the credit analysis department on the Agency's internal server in order to correctly and effectively perform their respective duties.

In addition, the files corresponding to the analysis reports, press releases, or rating letter will be sent to the persons authorized by the client to send and receive information, through the system the Company defines to protect non-public or confidential information.

The company maintains a clean desk policy and is strictly prohibited to remove files from the office. Employees are strictly prohibited from sending information for internal use to their personal email outside the Agency.

As part of the control measures to prevent the misuse of material non-public or confidential information, the computers of HR Ratings employees will be blocked from extracting information and introducing information via portable storage devices, such as removable hard drives, CDs, USBs, etc.

In the event any information contained on the Agency's internal server is required to be extracted to be stored on a portable device, or the extraction of information contained on a portable device to be introduced onto the internal server, the technical support team will be asked to intervene and perform this action using a computer thusly enabled. The technical support team may place the information extracted from a portable device on the internal server, after performing a security check.

Any extraction of information from the internal server or introduction of information onto the server will be duly documented in an information input/output log, indicating the name of the person, the type of file and information, and the date of the extraction (download) or introduction (upload). The Compliance Officer, with the support of the Chief Operating Officer, may audit these activities.

In addition, the Agency has a firewall in place to block access to personal email accounts by employees via public websites, therefore employees will only have access to email contained on the Agency's Outlook.

The Compliance Officer may conduct audits of the IT infrastructure to verify the firewall and blocking for the extraction of information on the Agency's computers are correctly implemented.

The analysis area is perfectly separated from the area of administration and business development. Additionally there is a separate area for visitors; this visitors area is an isolated area from analysis and the administration and business development areas.

Security for Electronic and Digital Information

Every employee of HR Ratings has a laptop computer setup with hardware and software to ensure security. As a consequence, all information regarding issuers, authorities, clients etc., is located in a “Secure Server” inside HR Ratings facilities with a full secure lock and only authorized personal can access.

The information stored in the internal electronic control and surveillance system and in the electronic folders of the HR Ratings’ internal server will be backed up daily. The backup and custody will be executed under the strictest conditions of security and confidentiality, in adherence of the disaster prevention procedure for electronic information, which is included in the Technological Infrastructure Protocol.

The Agency maintains the technological controls necessary to ensure the correct employee usage of the Internet and other means of communication. This includes prohibiting access to personal email and/or Internet sites that could present a risk to the Agency’s technological infrastructure.

These controls do not affect the sanctions that may be applied on the violation of the policies contained in this document.