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

HR Ratings treats all information it receives from an entity, issuer, or member of the issuer's o entity´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 Chief Compliance Officer is responsible for following up on the signing of these agreements and for overseeing ongoing compliance. The confidential information that entities or issuer´s 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, entities or issuer´s information will be sent solely to the person or persons designed as responsible for communication with HR Ratings and must be marked confidential.

To further protect private, non-public material information received from issuers or entities information received by e-mail is marked confidential and directed only to the persons authorized for this purpose.

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 entity or issuer file to complete their respective tasks, through the internal electronic system and the shared files on the Agency’s internal server for the control and follow-up of affairs.

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 members of the Compliance and Risk Departments will have full access to the client files on the Agency’s internal electronic control 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 entity or issuer to send and receive information, through the system the Company defines to protect non-public or confidential information.

The Company reports of private ratings are all marked as confidential treatment.

[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.

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.

The Company has a personal investment policy, applicable to all employees, which prevents the misuse of our clients' confidential information, and requires that all employees that have transactions with securities, submit a statement regarding the securities that they hold directly or indirectly in any entity or issuer rated by the company, as well as the statement of their spouse, partner or minor-aged children. The employees are required to notify the Chief Compliance Officer within 10 business days following the transaction in question, notwithstanding that all employees must submit the Appendix 1 of the Company's Code of Conduct every six months, accompanied with a brokerage or bank account statement in which, the securities transactions could be verifiable.

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.

The Compliance Department will train employees regarding the privileged information and its proper uses and disseminations. Also performs daily and ongoing tasks related to the development, adjustment, and administration of the internal control policies and procedures deemed necessary related to: the improper use of material non-public or confidential information; the handling and prevention of conflicts of interest; compliance with regulations applicable to credit rating agencies, and the handling of complaints.

Security for Electronic and Digital Information

Every employee of HR Ratings has a laptop computer setup with hardware and software to ensure security. Therefore, 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.

Policies and Procedures designed to prevent the misuse of material, nonpublic information and inappropriate dissemination within and outside HR Ratings of pending credit rating actions.

Material non-public or confidential information will be understood as all information received by HR Ratings from a client or member of the same business group, or from their accountants, attorneys, or other agents, that is visibly classified by the sender as material non-public or confidential, or regarding which the client has requested HR Ratings, in writing, hold confidential.

Material non-public or confidential information does not include that which has been made public through any action not imputable to HR Ratings prior to or at the time of its disclosure to HR Ratings. In addition, material non-public or confidential information will also not include information for which the client has given authorization for its revelation, or that which may be required by any authority.

The Chief Compliance Officer will be responsible for overseeing compliance with HR Ratings' policies on the prevention of the misuse of material non-public or confidential information by the Agency's employees, management and board members, for which compliance audits may be performed.

HR Ratings has established the following policies and mechanisms to ensure material non-public or confidential information provided by its clients is used solely and exclusively for the tasks of the Agency as a rating agency and to prevent the misuse of material non-public or confidential material.

The inappropriate dissemination within and outside HR Ratings of a pending rating action before issuing the credit rating on the Internet or through another readily accessible means is strictly prohibited.

To prevent favoritism in both time and quality, ratings and other rating actions, will be released the same day, to both the Mexican Stock Exchange, through the Electronic Sending and Dissemination of Information System ("SEDI"), to the Mexican Banking and Securities Commission through the Securities Information Transfer System ("STIV-2"), and to the general public through the HR Ratings website and any electronic communications network, such as Bloomberg and Reuters.