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

1. Material non-public or confidential information

Material non-public or confidential information will be understood as all information received by HR Ratings from an entity or issuer 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 entity or issuer 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 entity or issuer has given authorization for its revelation, or that which may be required by any authority.

The handling of and treatment given to material non-public or confidential information will be subject to that provided in this Exhibit and the non-disclosure agreements entered into between HR Ratings and the entities or issuers rated, between HR Ratings and its employees, and between HR Ratings and its vendors who may have access to this type of information.

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.

2. Measures to protect material non-public or confidential information

HR Ratings has established the following policies and mechanisms to ensure material non-public or confidential information 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.

2.1. Receiving information

HR Ratings may receive confidential information by email marked confidential and sent to any Agency employee authorized to intervene in the matter or who has been designated to this effect.

2.1.1. Protection of files and material non-public or confidential information

- All Agency employees and management who handle information provided by entities or issuers are obliged to adhere to the policies and guidelines for the

handling, protection, access and safeguarding of information and files, as contained in this Exhibit.

- All HR Ratings employees and management will clear their desks of information at the end of the workday and whenever they are away from their desk. They will also shred any documents no longer in use.

- Agency employees are strictly prohibited from removing papers or physical files or electronic files, containing material non-public or confidential information, from the Agency's offices.

- HR Ratings employees are strictly prohibited from transmitting, distributing, or sending information classified for internal use outside the Agency. Information for internal use is information provided by the entities or issuers or working documents containing material non-public or confidential information.

2.1.1.1. *Access to offices*

As an additional measure of protection for files and material non-public or confidential information, access to HR Ratings' offices will be restricted by fingerprint recognition, therefore visitors will be received in meeting rooms located in spaces that are physically separated from the Agency's operation.

The Senior Analyst, the Lead Analyst and the analysts that comprise the analysis team for a particular rating, may receive any type of information from the Client. Information may be received by hand in a sealed envelope directed to the relevant analyst, noting the date and time received, or may be received by email.

The Senior Analyst, the Lead Analyst and the analysts who assist them will treat all information received from the entity or the issuer as confidential, as per the terms of this Exhibit and in the non-disclosure agreement held with the Agency.

3. Access to client information and/or files

Only the Lead Analyst, the responsible Director and the support analysts assigned will have access to a client's file. To this effect, The Chief Credit Officer will assign and give access to the Senior Analyst or the Lead Analyst to a client, via the Agency's internal electronic system. The Lead Analyst can assign the Senior Analysist and other supporting analysist to a client.

When such is the case, on assigning the support analysts to a certain client via the Agency's internal electronic system, the Lead Analyst will automatically give the support analysts access to the client's file on the system.

In the event that during the course of the analysis process other personnel, in addition to the analysts designated require access to client files, the Senior Analyst or Lead Analyst will authorize access for such persons to the client files in question on the internal electronic system, via the system.

In addition, the Agency has a restricted access system to files containing information shared on the Agency's internal server, only allowing access to files and folders by employees who need access to these files due to their duties and assignments, no employee will access information that is not related to the matters in which they are involved.

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

The Compliance Department may conduct audits of the computers of HR Ratings employees, to ensure no employee has access to shared files for which they are not authorized.

In addition, as part of the policies to verify, accordingly, any misuse of material non-public or confidential information or privileged information, the Agency has a system to register persons that have accessed the shared documents and folders on the internal server, marking the date and time of the access.

Compliance and Risk Department personnel will have full access to the client files on the Agency's internal electronic 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.

4. Safeguarding Client information

Client files will be stored in an electronic folder on the Agency's internal electronic system and only the analysts assign will have access.

In addition, the work documents and other information will be stored in the protected folders on the Agency's internal server.

It is prohibited to store or hold confidential information on the computer's hard drive or on the desktop, meaning off the Agency's internal server.

Both the information stored on the Agency's internal electronic system and that stored in the electronic folders on 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 Agency's disaster prevention procedure for electronic information, which is included in the Technological Infrastructure Protocol.

The employees responsible for the security of electronic information inside the Agency will be held to the same rules of confidentiality and information handling applicable to the individuals involved in the rating process.

As a preventive measure, the people that provide the data backup and outside support services, and also those that, where applicable, provide scanning services for hard copies of information received from Clients will sign a non-disclosure agreement with the Agency, to ensure the proper handling of the information to which they have access.

Client files will be held for at least five years or the time establish by the applicable law, from the date on which the rating process in question is completed and will be available to the supervisory and regulatory authorities during this time.

a. Transmission or distribution of information

   Agency employees are strictly prohibited from removing any documents or electronic files containing non-public or confidential information from the offices of HR Ratings.

   In addition, HR Ratings employees are strictly prohibited from transmitting, distributing, or sending information classified for internal use outside the Agency, with the exception of communications with the Client concerned. Employees are strictly prohibited from sending information for internal use to their personal email outside the Agency.

   Information for internal use is that provided by the entity or issuer or work documents containing material non-public or confidential information.

   Client information will be sent solely to the person or persons the client has designated as responsible for communication with HR Ratings and must be marked confidential. The designated persons shall be updated in the internal control system.

   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 Agency defines to protect material non-public or confidential information.

   Analysts will only share information for internal use within the Agency with the members of the analysis team that is handling the matter in question.

Both the Agency and its employees, management, shareholders, and board members are strictly prohibited from disclosing ratings prior to their release through the corresponding means.

The Agency will release to the public through its webpage the ratings given on securities registered, or to be registered, in the national securities register, and the ratifications, amendments and/or cancellations of these ratings.

The ratings assigned by the Credit Analysis Committee will only be provided to the entity or issuer prior to being released through the corresponding media. Ratings requested by a third party involving the use of private information will be provided to the third party.

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 may audit these activities.

In addition, the Agency will have 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 working correctly.

*********