

KROLL BOND RATING AGENCY, INC.

Form NRSRO Annual Certification filed as of
March 31, 2017

<p>EXHIBIT 3: Statement of Policy on Confidential Information and Insider Trading</p>

POLICY STATEMENT ON
CONFIDENTIAL INFORMATION
AND INSIDER TRADING

**POLICY STATEMENT ON CONFIDENTIAL INFORMATION
AND INSIDER TRADING**

I. Introduction and Overview

Kroll Bond Rating Agency ("KBRA" or "the Company") provides independent analysis of financial products and institutions, including various credit rating services. In order to provide these services competently and effectively, the Company's employees will, from time to time, be provided with or have access to confidential information, which may include: (i) private information about clients, subscribers, and issuers and (ii) material, non-public information. Keeping private information confidential, and preventing any improper use of private information and material non-public information, are among the Company's primary operational goals. Accordingly, the Company has developed comprehensive policies to insure that it and all of its employees remain dedicated to these goals.

II. Types of Confidential Information

Information that is "confidential" is information that has been created or received by the Company in the course of its business activities, and is not generally publicly known or available. Confidential information can generally be described as "private information" or "material non-public information."

- A. Private Information – Information provided to an employee of the Company by a client, subscriber, or issuer that is not publicly available and which the client, subscriber, or issuer has not authorized the Company to make publicly available. This could include, but is not limited to, an investment strategy, portfolio holdings, proprietary information, financial projections, and market share information. In addition, information relating to the Company's business, such as proposed rating actions, non-public models and/or methodologies, or discussions of rating committee(s), must also be kept confidential. For example, a rating report that has not yet been published on the Company's website must be maintained as confidential until it is publicly disseminated.
- B. Material, Non-Public Information – Material, non-public information is any information provided to an employee of the Company that (a) would likely influence the average investor when deciding whether or not to invest in a given security; *and* (b) has not yet been disseminated in a manner that makes it generally available to investors, and/or the market has not yet had an opportunity to absorb such information.

Information is not confidential if it was publicly known at the time that it was received; and information ceases to be confidential if it becomes known to the public other than by an act of KBRA.

III. Procedures to Limit or Prevent Dissemination of Confidential Information

The Company and its employees shall take all reasonable precautions necessary to safeguard against both intentional and inadvertent dissemination of confidential information. The Company has implemented a number of policies and procedures to ensure compliance with this objective:

- A. Electronic Documents and Files – All employees' computers are password protected. Employees who have access to confidential electronic documents and files should log off or "lock" their computer at the end of each day, or whenever they are away from their desk or office area for an extended period of time. Additionally, the Company has developed an internal network that will enable a password-protected network drive to be dedicated to each project that entails the use of, or access to, confidential information that is received in connection with the credit rating process. The respective heads of departments (e.g., CMBS, RMBS, etc.) or project leaders will determine the access required by each employee, and will confirm the appropriate access levels to the Chief Technology Officer ("CTO"). Ratings analysts and ratings support staff should verify with the CTO which dedicated, password-protected network drive to use for a particular project, and should save and store electronic documents and files that contain confidential credit analytic information related to the project to that drive. Information that relates to fees (e.g., copies of engagement letters, correspondence related to fee structure, etc.) should be retained by marketing and relationship management personnel - - that is, personnel *other than* those involved in the ratings process - - and must be kept in a location that cannot be accessed by the ratings analysts.
- B. Hardcopy Documents and Files –
- *Warning Label* – Each employee who receives a physical document containing confidential information should immediately label it as such by either writing "CONFIDENTIAL" in a prominent place at the top of the page or affixing a label with the same warning in a conspicuous place. If the confidential information is contained on different pages within a file, packet, or binder, the employee may affix the warning label in a conspicuous place on the front cover or first page of the file, packet, or binder.
 - *Prevention of Unauthorized Access* – Employees should use their best efforts to prevent unauthorized persons from having access to confidential information at all times. Accordingly, employees should keep track of any documents containing confidential information that are removed from their desk or office area and should avoid leaving confidential materials unattended in common areas.
 - *Storage of Confidential Materials* – Ratings analysts and their support staff shall have access to a secure area where confidential material can be stored under lock and key. When confidential materials are no longer in use, ratings analysts and their support staff should ensure that confidential materials are retained in this storage area.

- C. Verbal Communications – Employees should only discuss confidential information on a “need to know” basis with other employees or third parties that are authorized to access the confidential information being discussed. If an employee is uncertain as to whether another employee and/or third party is also authorized to have access to such information, the employee should consult his or her supervisor. Typically, employees should not discuss confidential information with individuals that work outside of their department and/or are not working on the same project. Additionally, employees should use their best efforts to avoid discussing confidential information in a manner or setting where they may be overheard.

IV. Policy on Insider Trading

All employees are barred from trading on material, non-public (i.e., “inside”) information. In addition, employees are prohibited from “tipping” others (such as family members or friends) who could trade on the inside information. Any employee of the Company who comes into possession of material, non-public information, regardless of the source and whether or not the information pertains to an entity rated by the Company, is prohibited from discussing, disseminating, or acting upon that information in any way except during the course of the employee's legitimate business duties or where required by law. ***No employee may trade in any security while in possession of material, non-public information regarding that security. If an employee believes that he or she has received material, non-public information, or if there is any doubt about whether he or she is in possession of material, non-public information, the employee should immediately contact the Chief Compliance Officer or, in his absence, another member of the Legal or Compliance Departments.***

V. Maintaining Compliance

In order to promote and maintain compliance with the foregoing policies and procedures, the Company will distribute a copy of this policy statement to all employees and ensure that all employees know how to access it online. Additionally, a member of the Legal or Compliance Department will give periodic presentations to employees regarding the Company's policies and procedures for the proper handling of confidential information. All newly hired employees will also be given this presentation as part of their orientation.

In the event that any employee suspects that confidential material has been leaked, whether accidentally or otherwise, that employee should report such suspicion to the Chief Compliance Officer and his or her supervisor immediately.

If employees have any questions or concerns regarding the proper handling of confidential material, they are encouraged to see their supervisor and or a member of the Compliance Department - this includes any suggestions about how to improve these policies and procedures and any concerns regarding the improper handling of confidential materials. All supervisors and members of the Compliance Department shall have an open door policy when it comes to questions or concerns about confidential materials.

RESPONSIBILITY: CCO; CTO

Effective: 3/18/2011
Last Reviewed: 10/1/2012