Policy on handling Confidential Information

March 15, 2016
1. General provisions

This Policy on handling Confidential Information (hereinafter – Policy) was developed for the purposes of regulating main principles of work with Confidential Information defined in ACRA and of specifying ACRA employees’ responsibility for protection of its safety.

ACRA ensures safety of Confidential Information including information received from a Rated Entity, in the process of ACRA’s activity, as well as personal data, in accordance with requirements of the legislation of the Russian Federation and regulations of the Bank of Russia.

In order to ensure safety of Confidential Information ACRA uses organizational and technical measures.


The present Policy shall be posted on ACRA’s website www.acra-ratings.ru after it is approved by the Board of Directors.

2. List of terms and definitions

**ACRA** – Analytical Credit Rating Agency (Joint-Stock Company);

**Analytical Unit** – a set of ACRA’s Analytical Groups;

**Analytical Group** – an ACRA’s business unit performing such functions as analysis of creditworthiness of certain types of rated entities in accordance with the adopted Methodology as well as preparation and implementation of Rating Actions;

**Compliance Director** – an ACRA’s employee performing the functions of a comptroller (head of the Compliance and Internal Control Service);

**Confidential Information** – any information that is not generally available, including: (1) non-public information submitted by counterparties for Rating Actions in accordance with the signed agreements; (2) Material Non-public Information, obtained from any source; (3) details and plans for specific Rating Actions; (4) unpublished press releases regarding rating actions, unpublished reports on research and forecasts; (5) non-public information related to the work process of the Rating Committee; (6) details of agreements with counterparties for rating and other services; (7) internal non-public financial information; (8) a development strategy, description of internal business
processes and other know-how; (9) insider information according to the list specified by the regulation of the Bank of Russia; (10) personal data of ACRA’s employees and employees of corporate counterparties;

**Conflict of Interests** – a contradiction between ACRA’s proprietary and other interests and (or) those of its employees, and (or) Rated Entities/issuers, which may entail negative consequences for independence and/or objectivity of ACRA and (or) its employees;

**Non-public information** – information is considered non-public until it is spread in any way and by any means, providing access for the general public to this information;

**Rating Analyst** – an employee of ACRA’s Analytical Unit performing analytical functions required for Rating Actions;

**Rating Actions** – any of the listed events performed with regard to a Credit Rating of a Rated Entity: assignment, affirmation, review, approval and withdrawal, as well as assignment or revision of a Credit Rating forecast;

**Rated Entity** – a legal or a public-law entity whose ability to meet its assumed financial obligations (creditworthiness, financial accountability and financial sustainability) is explicitly or implicitly evaluated in an ACRA’s Credit Rating as a result of performed Rating Actions in relation to this entity;

**Material Information** – any information that can affect the value of public Securities, as well as information, which is material for investors when making their investment decisions concerning operations with Securities. The examples of Material Information for various companies are listed below:

- Information concerning planned assignment, modification, suspension of a Credit Rating or other Rating Action with respect to an issuer of securities or securities, accepted for an on-exchange trading or in respect of which an application for an on-exchange trading was submitted;
- Unpublished financial statements (audited / unaudited);
- Mergers and acquisitions, restructuring or asset sale/acquisition;
- Appearance or exit of a major supplier/customer/counterparty, significant changes in contract liabilities;
- Increase or decrease of dividends, split-up of shares/additional share issue;
- Changes of management structure/top-management positions;
- Potential legal proceedings.

**Security** – any traded financial instrument representing a traded asset.
3. Purposes of Confidential Information processing

3.1. ACRA and its employees must use Confidential Information only for the purpose of providing rating services or performing ACRA’s business activities.

3.2. ACRA’s employees must use Confidential Information received from Rated Entities, issuers, originators, underwriters or organizers, as well as the results of information analysis only for the purposes of formation of rating and other assessments as part of performing Rating Activities and rendering additional services.

3.3. ACRA shall reserve the right to use confidential statistical information of a Rated Entity without specifying the name of the Rated Entity in publications containing consolidated statistics if it is impossible for third parties to single out confidential statistical information from such consolidated statistics.

4. Restrictions when working with Confidential Information

4.1. When working with Confidential Information, ACRA’s employees are not allowed to:

- disclose (in full or in part) any non-public information concerning rating assessments, with the exception of a Rated Entity, issuer or their authorized representatives and cases, stipulated by requirements of the legislation of the Russian Federation;
- disclose (in full or in part) any non-public information concerning ACRA’s future Rating Actions;
- disclose (in full or in part) Confidential Information in press releases, during conferences, in conversations with potential employers, investors, other issuers and other persons;
- disseminate Confidential Information within ACRA, with the exception of those employees who need it for performance of their employment duties;
- distribute Confidential Information transferred by a Rated Entity or an issuer (originator, underwriter or organizer) between employees of companies affiliated with ACRA;
- use or disclose Confidential Information received from Rated Entities, issuers, originators, underwriters or organizers in violation of conditions of its transfer to ACRA, with the exception of cases, stipulated by requirements of the legislation of the Russian Federation.
5. Distribution of employees’ rights of access to Confidential Information

5.1. When distributing employees’ rights of access to Confidential Information ACRA shall be guided by the following principles: “Know Your Employee” and “Need To Know”.

5.2. “Know Your Employee”: the principle reflecting ACRA’s concern over employees’ attitude toward their obligations and over their potential personal problems, including financial problems, breach of law, etc., which can lead to occurrence of a Conflict of Interests.

5.3. “Need to know”: the principle, limiting access of an ACRA’s employee to Confidential Information and IT-resources processing this information to the minimum level required for performance of his/her employment duties.

5.4. ACRA classifies Confidential Information as well as its employees according to their types and categories and approves internal documents, regulating rules of access of different categories of users to various types of Confidential Information.

5.5. Internal documents regulating Confidential Information access rules stipulate in a mandatory manner creation of a “Chinese wall” separating Confidential Information of the Analytical Unit and Confidential Information of ACRA’s departments responsible for advertising, client acquisition and conclusion of Rating Action agreements as well as corresponding access settings for ACRA’s employees.

6. Main requirements to ACRA’s employees when handling Confidential Information

6.1. For keeping Confidential Information safe ACRA’s employees are obliged:
- to fulfill requirements of all ACRA’s internal policies and documents which regulate protection of Confidential Information;
- to take all reasonable measures to protect all available Confidential Information against fraudulent actions, theft, illegal use or unintentional disclosure;
- to refrain from discussing or transferring Confidential Information to ACRA’s employees who are not granted an access to this information and to other persons (in ACRA’s office and beyond);
- not to disclose Confidential Information obtained from ACRA’s clients to third parties without a client’s written consent or at the request of authorities of the Russian Federation;
• to use only ACRA’s IT-resources for storing Confidential Information;
• to use only ACRA’s internal e-mail for exchanging Confidential Information within the framework of their employment duties (with other ACRA’s employees and external counterparties);
• to keep their personal passwords secret and to ensure safety of their laptops, smartphones, removable data storage media and smart cards;
• to refrain from discussing Confidential Information between themselves in public places where this discussion can be heard (incidentally or deliberately) by third parties;
• to exclude Confidential Information from disclosure including in the course of preparing analytical reviews, participating in panel discussions and at forums;
• not to leave Confidential Information in paper format (documents) in common areas (in ACRA’s office and beyond);
• to ensure safety of documents containing Confidential Information if ACRA’s employees, who do not have a permit to work with this information, or other unauthorized persons have an access to the desk of an employee working with Confidential Information. At night, the documents must be put in the employee’s drawer, cabinet or safe; during the day it is allowed to leave documents on the desktop face down.

7. Informing about non-compliance with the requirements of this Policy

When receiving data that an ACRA’s employee has committed (is committing) illegal, unethical actions or those that violate this Policy or when there are reasonable suspicions that such actions have been committed, every ACRA’s employee must report such information to the Compliance Director.

ACRA considers any failure to provide information about another ACRA’s employee committing illegal, unethical actions or actions that violate this Policy or ACRA’s internal documents as complicity in such an action.

8. Final provisions

ACRA shall undertake all required measures to prevent violation of requirements of this Policy by ACRA’s employees.
Failure to comply with requirements of this Policy can result in disciplinary action against an employee, up to and including termination of employment.

Any deviations from this Policy should be documented in writing and agreed upon by the Compliance Director and the Board of Directors pursuant to the procedure established by ACRA’s internal documents. Any deviations from this Policy resulting in a breach of requirements contained in government regulations of the Russian Federation and requirements of the Bank of Russia are not permitted.

This Policy shall come into force after 7 business days from the moment of its approval by the ACRA’s Board of Directors and shall be valid until approval of an updated or substituting document.