Information Security Policy

ÓRIA

ÓRIA GESTÃO DE RECURSOS LTDA.

October 30, 2018

INFORMATION SECURITY POLICY

1. Introduction.

ORIA GESTÃO DE RECURSOS LTDA. ("ORIA") is a Private Equity & Venture Capital (PE&VC) investment manager with exclusive focus on Information Technology (IT) assets in privately-held companies with no stock market value and with restricted liquidity.

ORIA engages exclusively in securities portfolio management activities duly registered in the category set forth in paragraph 1, item II, of CVM Instruction 558 of March 26, 2015 ("CVM Instruction 558/15"), managing Private Equity Investment Funds ("Funds") regulated by CVM Instruction 578/16, which funds have outsourced fiduciary administration and custody.

1.1 Objective.

This Information Security Policy aims at providing information to ORIA Employees in order to alert them and guide them regarding the legal care required as far as Information Security is concerned, thus ensuring the appropriate controls in the information management.

1.2 Concept.

Information Security refers to the existing protection of information concerning ORIA and its Clients.

Information is understood to mean any and all content or data that is valuable to any organization or person. It may be stored for restricted use or available to the public for consultation or acquisition. Information makes up one of the main assets of ORIA, being a quality information flow capable of deciding the success or failure of an enterprise. This power, added to the increasing easiness of access, makes this "asset" a target of constant internal and external threats ("Risks").

Thus, this Information Security Policy should be seen as the foundation of the efforts to protect ORIA´s information, always with due regard to the following criteria:

• **Confidentiality** - limit access to information only to legitimate entities, that is, those authorized by the owner of the information.

• **Integrity** - property that ensures that information processed maintains all original characteristics set by the owner of the information, including control of changes and assurance of its life cycle (birth, maintenance and destruction).

• **Availability** - property that ensures that information is always available for legitimate use, ie. by those users authorized by the owner of the information.

1.3 Risks.

Improper management of Risks can cause irreparable damage to ORIA, and the absence of adequate controls are as follows:

• **Loss of Confidentiality**: when there is a breach of confidentiality of certain information (eg, the password of a user or system administrator) allowing restricted information to be exposed which would be accessible only by a certain group of users.

• **Loss of Integrity**: When certain information is exposed to handling by an unauthorized person, who makes changes that have not been approved and are not under the control of the owner of the information.

• **Loss of Availability**: when the information is no longer accessible to those who need it. This would be the case of the loss of communication with an important system for the company, which would happen with the outage of a server, or of a critical business application, that presented a failure due to an error caused by reason internal or external to the equipment, or by unauthorized action of persons with or without malice.

2 Security Devices.

Physical access passwords: All employees must generate individual access passwords for the electronic door entry, according to procedures distributed by the Administrative Management of ORIA. Passwords created are individual and non-transferable. In case of dismissal of any employee, the administrative manager will be responsible for disabling his/her access immediately after the dismissal.

Control and storage of physical documents: Physical documents characterized as restricted access and confidential are kept indoors and with access permitted only to authorized persons:

a. Control of deposit and withdrawal of documents restricted to ORIA employees.

b. The availability of documents must be assured by a careful process from the moment of archiving, appropriate location criteria, among other processes considered to be necessary.

Restricted access and secret documents are considered to be:

I. Financial statements;
II. Contracts with third parties;
III. Contracts, minutes and other corporate documents.

Control of access to online systems and repositories: Access to these ORIA systems is controlled and limited to its Employees. Access is allowed per user, with differentiation of access profile (segregation of functions) through password. The

password is personal and non-transferable and includes double checking devices via sms or email. In addition, passwords should be updated by users from time to time every 120 days.

Any change or authorization of access should be sent to the IT manager with a copy to the Compliance officer.

The use of e-mail programs, or "e-mails", should be exclusively for professional scope messages, as they carry the identification of the company to the environment of the worldwide network of computers. Under no circumstances may such message exchange systems be used to transmit or retransmit messages that could endanger the name of ORIA, especially those carrying texts or attachments that may be considered offensive.

The use of private e-mails (such as, GMAIL, Terra, UOL, etc.) for corporate use is not allowed.

ORIA's mobile computer systems should be used exclusively for the professional activities for which the employee has been hired. The category of mobile computer systems includes notebooks, modems, smartphones and tablets. Any other so-called "application systems" or "software programs" that do not have the proper license or even the proper approval formally granted by ORIA shall not be installed, processed or used in all mobile computing devices.

The inclusion of profiles in ORIA management systems qualifies the user to use all the resources of the systems authorized by the Systems Administrator and the Management to which the user is subordinated. Upon its inclusion, the user will automatically be subject to the rules of use of ORIA.

The Management, to which the user is subordinated, is responsible for defining the assignments, authorizations, maintenances, suspensions or definitive cancellation of profiles with the System Administrator.

All employees should, when absent from their workstation, block it, aiming at complying with safety measures and reducing energy consumption. Being absent means the fact of leaving the workstation, regardless of reason or time, without personal monitoring of each user.

All documents generated in ORIA's internal processes are considered as confidential and undue disclosure of any information contained therein must be avoided.

To ensure the confidentiality of printed information, it will be fragmented to prevent its reading.

ORIA does not internally process any application related to company routines. In contracts involving the processing of confidential data, clauses should be included to deal with the necessary care for the confidential treatment of this information by compelling ORIA's counterparties to comply with this Information Security Policy.

ORIA has a System Administrator in place, which is assigned with the mission of ensuring the most efficient support to the needs of the business generation processes. Monitoring report of T.I. is sent to the Compliance Officer on a weekly basis.

3 Information Secrecy.

This Information Security Policy is also intended to comply with the BACEN determinations in MNI-02-01-14 dealing with banking secrecy that specifies: "*Securities brokers and securities dealers must maintain secrecy of their transactions and services provided, disclosing information only upon written authorization by their clients.*" (Res. 38 XII b, Res.1120 RA Art.13, Res.1655 RA Art.13, and Res.170 RA Art.10) ("Information Secrecy").

A client´s name and transactions should not be informed unless by order or written request of the Central Bank, the CVM, Stock Exchanges or court authorities, in those cases provided for in the applicable laws.

Application: this Information Security Policy will apply to:

a) All ORIA Employees;
b) The dealer hired to distribute the funds under the management of the manager;
c) The self-employed agent hired to distribute the funds under the management of ORIA; and
d) The former employees who will be under the obligation to comply with the terms of this Policy for the period established herein in the same manner as when they were active Employees of ORIA.

In the distribution of funds to clients: in order to minimize image risks, since clients can link ORIA´s name to a possible failure that may occur in their information, it is recommended that managers discuss the Privacy Policy of those dealers with which they will make their funds available and that the distribution agreements ensure privacy to the clients that purchase the funds managed by ORIA.

Daily routine:
Employees while occupying a position of trust in ORIA, and even after leaving the company, shall protect the confidentiality of any information which ORIA Employees may have access to as a result of performing their functions in ORIA, including through the systems and files made available by ORIA for that purpose, which are notoriously and provenly not in the public domain ("Confidential Information"). Among such information are:

- Operations, strategies, results, assets, data and projections that may lead to a competitive edge of ORIA over its competitors;
- Information about the ORIA business plan;
- Confidential information about ORIA Employees; and
- Information about customers, distributors and suppliers.

Sensitive issues involving ORIA matters should not be discussed in public venues such as corridors, elevators, public transportation, restaurants, etc. The company's internal email is controlled, and messages can be tracked by the Compliance officer in case of any suspected violation of ORIA Policies, Rules and Procedures.

For former Employees:

A former Employee is not allowed, for a period of 02 years, to use the information obtained during the exercise of his/her activities with ORIA, of any content whatsoever, whether this information is confidential or not, for his/her own benefit or for any other reason, even though to the benefit of ORIA itself.

If ORIA is aware of the leakage by a former Employee of Confidential Information or of an attempt to tarnish the image of ORIA before its clients, in order to cause him or her to cease being a client, the professional may be criminally and civilly sued for his/her acts.

Likewise, Employees should avoid keeping confidential papers and documents on their desks. Confidential documents should be kept in an appropriate place and locked, even during business hours, in order to prevent access by unauthorized third parties. At the end of the day, the desks should be free from papers or documents.

IT security: ORIA does not use internal networks or virtual machines by eliminating an additional vulnerability point within its information security control. The company relies on the information security afforded in applications, systems and online file repositories delivered in the Software as a Service model, in which large vendors, such as Salesforce.com Inc. (NYSE: CRM), have investments and specialization in information security at a magnitude infinitely greater than a resource manager can have.

The IT officer conducts timely monitoring of the use of the ORIA systems by their users in order to identify improper accesses and ensure the security of the information recorded in those systems. The internet links are redundant, with the connection via NET of 20 Mbps and Vivo 60Mbps.

ORIA makes use of anti-spam to block malicious e-mail messages, the use is linked to Microsoft's own system and the Exchange online technology that tracks the incoming and outgoing emails on the internet server.

The ORIA firewall is based on iptables that block improper access to the network through the SuSE-Firewall System.

As the leading antivirus software, ORIA makes use of Microsoft Security Essentials. The software is daily and automatically updated, and performs weekly scans in search of any software that could endanger the entire IT structure of the company.