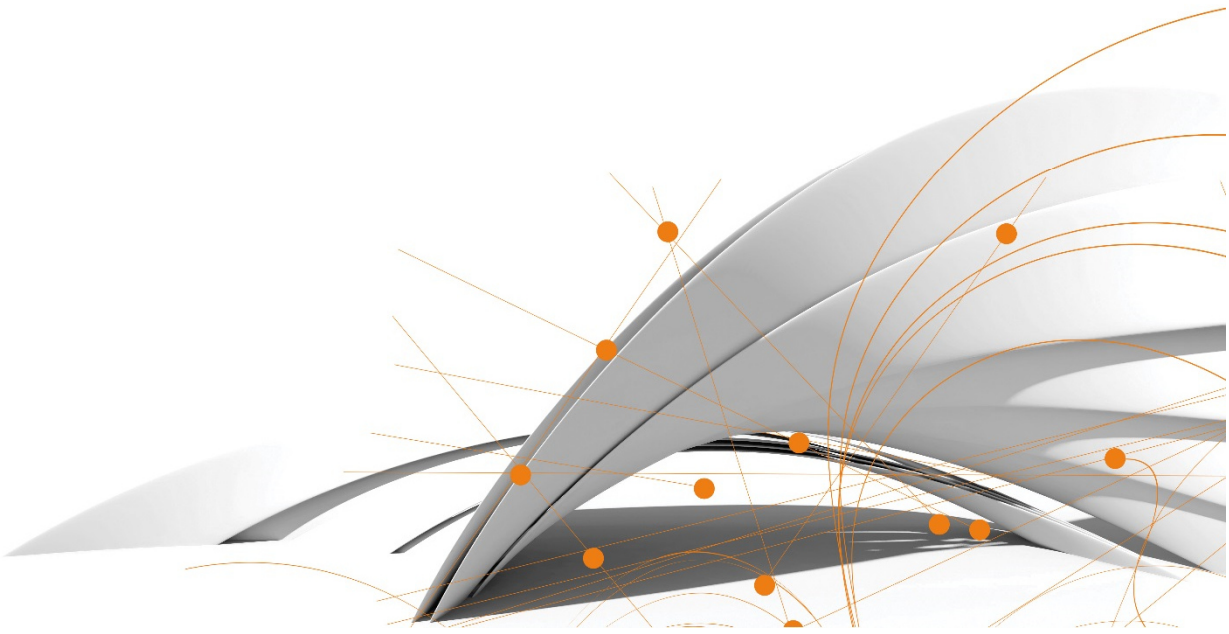
TOBAM

CORE INVESTMENTS

Privacy policy



I. Introduction

TOBAM and its affiliates ("the Company") are committed to responsibly handling information regarding its investment advisory clients and investors in the funds it advises ("Funds"). New technologies have changed the way information of all kinds is gathered, used and stored, but the importance of preserving the security and confidentiality of investor information is a core value of the Company.

The protection of client information is of the utmost importance. All employees and directors must ensure that all client information is protected from unauthorized use or disclosure.

II. Guidelines to ensure you maintain the privacy of client information

1. You MUST:

- Keep client information confidential. Use reasonable efforts to limit access to records containing client information to personnel who has a need to know the client information in connection with the Company's legitimate business purposes or to comply with the law;
- Include in emails only necessary client information and send such emails to the smallest distribution necessary under the circumstances;
- Hold meetings with clients and other third parties in conference rooms or other locations where client information is not generally available or audible to others;
- Use reasonable efforts before responding to requests for client information from third parties to guard against fraudulent requests;
- Properly dispose of documents and electronic records that contain client information such that client information contained therein is destroyed, erased or otherwise rendered unreadable;
- Keep confidential and secure user IDs and passwords for access to computers, files and portable devices such as cell phones, USB flash drives, portable hard drives, backup tapes and laptop computers;
- Keep under your control or the control of another authorized personnel or service provider at all times records, laptops and portable devices containing client information that are transported outside business premises;
- Keep confidential and secure access cards and access codes for Company offices;
- Immediately report lost or stolen Company electronic storage or portable devices.
- Obtain prior approval from the Legal and Compliance department to share client information with third parties that are not affiliated with the Company unless it is: (i) requested by or with the consent of the client; or (ii) necessary to enable the Company to maintain or service the client's account.
  If you are uncertain whether client information can be given to a third party, you should ask the Compliance Officer for guidance.
- Account for visitors in the offices. A visitor should never be left alone in the office and the person opening to the visitor is responsible for requesting the name of the visited person and accompanying him/her to the visited person. The visitor is then under the responsibility of the visited person.

2. You MUST NOT:

- Leave documents containing client information in office areas where unauthorized persons can read them, such as in photocopying areas, conference rooms or other common areas, overnight on desks in unlocked offices, or in unlocked cabinets or other unsecured areas;

- Store or download client information or emails that contain client information on or to any computer or portable device that is not issued to you by the Company ("non-Company devices"), including any home computer. You may access and/or email client information from non-Company devices only via a secure connection;

- Access client information on any computer or portable device through an unencrypted network;

- Tamper with or disable any encryption, firewall or system security software installed on any Company-issued computer or portable device; and

- Share any client information with terminated employees, or provide terminated employees with access to any client information.