Julius Bär

Julius Baer Capital (India) Private Limited

Vigilance mechanism

Purpose

Julius Baer's reputation for integrity is one of its most important assets. Trust and credibility are absolutely essential for the Julius Baer Group (the "Group"). One key aspect of trust and credibility is compliance with laws and regulations. To protect and maintain this reputation, employees must not only follow the laws and regulations and the Group's own rules and regulations, but are encouraged and expected also to report cases of (suspected) misconduct (including violations of policies) of a legal, regulatory or ethical nature.

The Group has a legitimate interest in misconduct being reported internally so the misconduct can be addressed and corrective action can be taken.

The Companies Act, 2013 requires every company which has borrowed money from banks and public financial institutions in excess of fifty crores to establish a vigil mechanism for their directors and employees to report their genuine concerns or grievances. The borrowings of Julius Baer Capital (India) Private Limited (JBC) are in excess of INR 50 crores and as such, the need for such mechanism.

Scope

This Policy is for the Directors on the Board of JBC and all internal and external employees (agents) of JBC to report genuine concerns or grievances.
This policy should be read in conjunction with the Fraud Monitoring Policy of JB Capital (India) Private Ltd.

Minimum Standard

The policy contains at least the following:

- Reportable incidents / case categories (if deviating from this policy)
- Other reporting channels
- Responsibilities of the case managers
- Usage of data upload
- Data privacy
- Case management
- Access permissions
- Reporting
- Additional requirements

Reportable incidents

Directors and employees should report suspected misconduct relating to the following:

- Threats, stalking
- Theft, vandalism, damage to JBC's property
- Embezzlement, fraud, disloyal management of business
- Accounting fraud
- Information security breaches

- Money laundering, terrorism
- Bribery, corruption
- Improper behavior, bullying, harassment
- Conflicts of interest
- Environmental pollution
- Misconduct with regard to community engagement activities
- Other, miscellaneous

Personal or personnel matters other than defined above are not considered as reportable incidents in accordance with this policy and should be submitted directly to Human Resources ("HR"). If the directors and employees do not want to discuss the matter with HR, then they can approach the CEO or Local L&C.

The reporting system is not for reporting emergencies, alerts or cases of immediate danger. Such incidents have to be reported directly to the Line Manager or CEO/COO/CRO/L&C/HR/ Corporate Services

Committee

The Company's Audit Committee shall oversee the vigil mechanism.
If any members of the committee have a conflict of interest in a given case, they should recluse themselves and the others on the committee would deal with the matter on hand.
This committee shall also be responsible for assigning the case to a Case Manager and ensuring appropriate response/communication are provided to Reporting Person, Regulators, Press, Clients, etc.

Reporting system / process (JB Integrity Platform)

As a first channel of reporting, employees shall report a Reportable Incident to their Line Manager.
In case this is not possible (e.g. in case line management is possibly involved in the misconduct themselves), then the next channel of reporting should be to COO/CRO/L&C/HR
If this proves not to be effective or if other prevailing reasons create a preference for the employee to make use of the reporting system, then the employee shall send a letter addressed to the HR (or) L&C (or) CEO. Although Julius Baer maintains an open corporate culture and encourages employees not to report violations anonymously it is left to the employee whether to disclose his/her name or not in such complaints. Incidents reported through such letters shall be forwarded by the recipient to the Audit Committee and also documented in an Incident Register. Collectively a Case Manager will be identified to handling such Reported Incident.
In appropriate or exceptional cases, the victim would have direct access to the Chairman of the Audit Committee of the company.

The Reporting persons may request information with regard to their report at any time. However, the outcome and result of the investigation in certain cases must not be reported back due to data protection and privacy reasons. The Reporting persons shall receive a brief generic update/feedback from the Case Manager on the status of the action taken on the reported incident, within 10 working days.
Subsequently, a generically worded update may be provided, by the Case Manager, upon completion of the internal investigation. The wording of these notifications will be determined by the respective Legal department.

All Reported Incident should be investigated and completed within 30 days of receipt of such reporting.

Confidentiality

Julius Baer expects its employees to report misconduct and wrongdoing based on reasonable indications. Any such reporting in good faith through the above mentioned channels will as a consequence not lead to negative consequences for the reporting person (unless such person is himself/herself involved in the wrongdoing/misconduct, in which case however, such reporting will be taken into consideration) or victimization of the reporting person.

In case of repeated frivolous complaints being filed by a director or an employee, the audit committee may take suitable action against the concerned director or employee including reprimand.

Any report to third parties such as to law enforcement agencies, the press etc. need to be channeled through the responsible specialist teams e.g. Legal and/or Compliance, Communication and the like. Autonomous reports may lead to negative consequences for the reporting person. In particular the latter could constitute an illegal disclosure of business secrets and information protected by data protection and privacy/confidentiality laws (including banking secrecy) and would destroy the basis (trust) for a continuation of the employment.

Case management

Cases are principally investigated by the following departments depending on the reported case category:

- Global Personnel & Physical Security
- Global Fraud Prevention & Detection
- Information Security
- Internal Audit
- Legal and/or Compliance
- Human Resources
- Corporate Social Responsibility
- Global Corporate Services
- Group General Counsel Office

Cases are automatically assigned to a case manager by the category of the case as listed in section 3. Reports that meet the criteria for two or more categories based on the case type/subject matter are assigned to a case manager according to availability, independence and specialization. In addition, a re-assignment of a case to another category remains reserved.

Reporting Structure

- Upon completing the internal investigation, investigating case managers must prepare a case report to the attention of the Audit Committee.
- The Audit Committee shall take a decision whether to report it to the Board of JBC and also to other internal stake holders regionally and globally.

Implementation date

This policy enters into effect as of 23.2.2016.