Whistleblowing Policy

EXCLUSIVE NETWORKS

Table of Contents

I. Introduction **2**

1.1. Objectives 2

1.2. Review 2

II. Scope **2**

III. Matters to report under the policy **3**

IV. Raising Complaints **4**

V. Treatment of Complaints **4**

VI. Investigation process of Complaints **5**

VII. Confidentiality and protection from reprisals **6**

VIII. Retention of personal data **6**

IX. Effective Date **7**

I. Introduction

1.1. Objectives

This policy aims at operating on a highly transparent basis. The company wants to be aware of significant wrongdoings and address them as soon as possible. All complaints or concerns regarding accounting, legal matters, fraud or non-compliance may be addressed through this Policy.

The aims of this Policy are:

i. to make employees aware that:
   - genuine and reasonable suspicions of illegal or unethical activities, or inappropriate practices, should be reported as soon as possible;
   - any concerns will be taken seriously;
   - any concerns will be thoroughly investigated, and action taken as appropriate; and
   - confidentiality will be respected;

ii. to provide employees with guidance as to how to raise any concerns; and

iii. to support employees and reassure them that:
   - they are able to raise genuine and reasonably held concerns in good faith, even if they turn out to be mistaken; and
   - they will be protected against reprisal and retaliation.

For the avoidance of doubt, the aims listed above apply equally to third parties who wish to make a report.

1.2. Review

The Whistleblowing Policy will be reviewed when needed by the Risk and Compliance Department and any amendments will be incorporated accordingly.

II. Scope

The Whistleblowing Policy is designed to enable any employee or any third party (reseller, end-user, vendor, service provider, distributor, etc.) to make fair and prompt disclosure of any concerns where they genuinely and reasonably believe that the high standards expected in Exclusive Networks have not been met.

This policy does not seek to replace the communication of concerns or the raising of questions or issues by employees or third parties to supervisors, Risk and Compliance Department, Ethics Champions, Human Resources or otherwise as appropriate. This is an additional communication channel that may be used to report significant matters.

For the purposes of this Policy, the term "employee" means employees (whether fixed term, permanent or temporary), directors, officers and other individuals working for Exclusive Networks such as contractors and professional service providers.

The term "the Company" refers to any subsidiary of Exclusive Networks, as well as the Holding companies.

III. Matters to report under the policy

Any information which relates to suspected activities or practices which fall below the highest standards of business conduct and personal behaviour as expected by the Exclusive Networks Code of Conduct should be disclosed under the Policy. This may include:

- Intentional error, fraud, negligence in the preparation, review or audit of any of the Company's Financial Statement or in the recording of the Company's Financial records;
- Intentional noncompliance with company policies or with the applicable laws;
- Any suspected fraudulent activities (such as but not limited to bank fraud, money laundering, fraudulent statements to management, fraudulent use of access rights, unlawful agreements with competitors, unlawful working conditions, tax fraud, etc.);
- Violations of the Anti-Corruption Laws (FCPA, Loi "Sapin 2", UK Bribery Act or similar laws);
- Violations of the Code of Conduct (for example, corruption, discrimination, harassment);
- Crime, misdemeanours, serious threat or harm to the general interest.

The above list is not exhaustive, and no one should be discouraged from making any disclosure of concerns that they may have simply because those concerns do not fall within the categories identified above. If in doubt, employees should communicate their concerns to your respective line managers or with Human Resources.

IV. Raising Complaints

All complaints received will be treated confidentially.

Any Complaint can be raised via:

- Our external whistleblowing platform at: https://exclusivenetworks.integrityline.com;
- Email using the address Ethicspoint@exclusive-group.com;
- Regular Mail to Exclusive France Holding – Group General Counsel - 20 quai du point du jour – 92 100 Boulogne-Billancourt- France.

When using the external whistleblowing platform, the whistleblower will have the possibility to remain anonymous throughout the entire process, to the fullest extent legally permitted in his/her local jurisdiction.

Raised complaints must include:

- A clear description of the facts or concerns;
- The entity name;
- Where necessary and possible, information on the sources of information, consequences and impacts.

Anonymous alerts will be treated only if the facts described are provided with enough detail.

V. Treatment of Complaints

Exclusive Networks will arrange for the proper and appropriate investigation of any disclosures made by any employee or third party under and within the scope of the Policy. Investigations will be conducted promptly and fairly, with due regard to the nature of any allegations and the rights of the individuals subject to the concerns.

Depending on the nature of the concern the Risk and Compliance Department may involve an appropriate external body which will be required to comply with the relevant Data Protection legislation.

The person appointed to investigate the concern will be independent, without any:

- Direct interest in the subject matter;
- Conflict of interest with the individual making the disclosure (if not anonymous), or with any other involved individual.

Through the whistleblowing platform:

(https://exclusivenetworks.integrityline.com/frontpage), the employee/third party will be able to login at any time (on a confidential basis, using the incident number provided when submitting the report and a defined password) to track the status of the investigation. As such, he/she will be able to see whether the alert has been acknowledged (with the date and time of the acknowledgement), whether the investigation has been launched and if so when, and what is the status of the investigation. Through the platform, the investigation team will be able to:

- Ask any further question using an encrypted dialogue functionality on the platform;
- Provide feedback to the individual making the disclosure (within a reasonable period of time not exceeding three months).

If any investigation concludes that an employee has made false concerns in bad faith, that employee's conduct may be sanctioned for failing to uphold Exclusive Networks commitment to openness, honesty and integrity in the workplace.

VI. Investigation process of Complaints

Received complaints will be logged into the whistleblowing platform. This will include the date of the complaint, description, submitter if non-anonymous, status of the investigation, and conclusions.

The Risk and Compliance Department will ensure coordination of the treatment of the complaints and may report immediately the significant items to the Audit Committee. A quarterly reporting will be communicated to the Audit Committee with complaints received and updates on pending investigations. Access of reports to third parties will be at the discretion of the Group Compliance Officer.

When appropriate, complaints may be transferred to an appropriate person or department to be investigated unless the complaint involves this specific person or department. Complaints will be anonymized before being transferred internally (in the case the platform was not used anonymously). Confidentiality will be maintained to the fullest possible extent. If confidentiality is compromised, disciplinary sanctions may be taken against the person who has breached confidentiality or the anonymity of the whistleblower.

Individuals who are the subject of the complaint will be informed about the ongoing treatment of the alert once first investigations are initiated (in order to protect against the loss of evidence). This is also to provide them with the opportunity to oppose the treatment of the case for a legitimate reason (false accusation or scurrilous allegation for example).

Anonymous alerts will be marked as such in the communications made during the related investigation.

Prompt and appropriate corrective action (including disciplinary action up to termination of employment) shall be taken as determined by the Risk Committee and depending on the nature and gravity of the conduct or circumstances. The matter may be reported to the police or any other competent authority, or a lawsuit filed, if deemed necessary.

Please refer to Exclusive Networks Fraud and Investigation policy for further details on the investigation process.

VII. Confidentiality and protection from reprisals

Exclusive Networks is committed to ensuring that employees feel able to raise concerns openly in good faith under the Policy, without fear of reprisal or retaliation and with the support of Exclusive Networks.

Where an employee genuinely believes that there is some form of wrongdoing or danger at work and a concern is raised in accordance with the Policy, Exclusive Networks will take all reasonable steps to ensure the employee does not suffer any disadvantage in the workplace as a result of speaking up about their concerns. Employees who believe that they have been subjected to such reprisal, threats, retribution or retaliation may raise the case to the General Counsel. On the contrary any bad faith complaints raised may lead to disciplinary actions against the submitter.

If a concern turns out not to be well founded, provided that it was raised in good faith and the employee did not commit any misconduct collecting evidence regarding their concern, Exclusive Networks will take all reasonable steps to ensure there is no disadvantage in the workplace suffered as a result of speaking up, nor will an employee lose their legal protection as a result.

Exclusive Networks will seek to carry out its investigations in a confidential and sensitive manner, and the number of persons involved and who are aware of the details of the concerns, including the identity of the employee raising the concerns, will be kept to a minimum.

VIII. Retention of personal data

Any personal data will be collected in strict compliance with Exclusive Networks Global Privacy Policy, only to the extent that is legally permitted and appropriately related to the investigation. Such personal data may be retained until the end of the investigation or,

when applicable, until any proceedings have been decided or until legal remedies have been exhausted.

Communications and documents related to alerts that did not lead to any disciplinary or legal actions will be deleted or archived after being anonymized within two months after the case is closed. Cases leading to further disciplinary or legal actions will be archived as per legal requirements

Alerts that are out of the scope of this policy will be deleted immediately or anonymized. The anonymization procedures used should comply with the recommendations of the 05/2014 opinion on anonymization techniques of the European Data Protection Committee (avis 05/2014 relatif aux techniques d'anonymisation du Comité Européen de la Protection des Données).

When no action is initiated in response to an alert within the scope of this policy, personal data are destroyed or anonymized within two months from the end of the review or investigation process.

In the event that disciplinary or litigation proceedings are initiated against a person involved or the author of an abusive alert, the data relating to the alert may be retained until the end of the proceedings or the time limit for appealing against the decision.

IX. Effective Date

This Policy comes into effect as of October 29, 2021. It supersedes and replaces any other guidelines or policies of Exclusive Networks to the extent that they pertain to Whistleblowing.