Whistle-blower Policy

Whistle-blower Policy

Contents

Policy details

Policy Exco owner	Chief Financial Officer
Policy owner	Head of Internal Audit
Approval body	Level 2 - MB on recommendation of Exco (material changes); Policy owner (non-material changes)
Policy scope	Global (all employees)
Policy classification	Low (3 year revalidation)
Data classification	Public
Supporting learning modules (ELLA)	None
Supporting documents	Whistle-blower Procedure

Version control

Version	Publication date	Approved by [Name][Date]:	Version changes
5	20211118	CFO, 9 November 2021	Updates to comply with Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (Whistleblower Protection Directive)
4	20210728	SB, 28 July 2021 (with effect of 1 July 2021)	Split Audit & Risk Committee into two separate committees with effect of 1 July 2021: references in the Global Procedure to 'Audit & Risk Committee' changed to

			'Risk Committee'
3	20201126	MB, 26 November 2020	Periodic revalidation and update to new Policy House framework - no material changes
2	20170823	MB, 23 August 2017	Periodic revalidation
1	20151002	MB, 2 October 2015	New Policy

1 Background and purpose

1.1 The purpose of this Policy is to provide all Intertrust Group Employees (as defined below) with a mechanism for reporting Concerns (as defined below) outside of the normal management reporting channels.

2 Scope

2.1 This Policy applies to all Intertrust Group offices globally and to all Employees and Third Parties (as defined below) and should be regarded as the minimum group standard requirement.

2.2 An Intertrust Group office may, subject to approval by the Head of Internal Audit, apply a local addendum to this Policy to accommodate the requirements of local law and/or regulation. Any local addendum should follow the spirit of the control environment described in this Policy and deviate only so far as is required to meet the specific requirements of the law/regulation.

2.3 A request for approval should be accompanied with a proposal for the content of the local addendum, approved by the Local and Regional Governance, Risk & Compliance (**GRC**) Head, and must be sent to the Head of Internal Audit accompanied by a detailed justification of why this is required.

2.4 HR grievances are not part of the scope of this policy and are dealt with by HR policy.

3 Definitions

3.1 *Definitions*

Boards - means the Management Board or the Supervisory Board of Intertrust N.V.

Concerns - means a suspicion of or actual knowledge of any of the following behaviours in a work-related context:

(a) questionable or improper accounting or processing matters;

(b) violations of Intertrust's policies;

(c) breaches of regulatory requirements;

(d) illegal and/or dishonest activities; or

(e) any other wrongdoing at work.

Employee - means an Intertrust employee that can report via the (internal) reporting channels.

Third Party - means a third party that can report via the (internal) reporting channels, including:

(a) contractors;

(b) shareholders (and people belonging to the Boards);

(c) persons working under the supervision and direction of contractors, subcontractors and suppliers;

(d) former employees; or

(e) reporting persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

Whistle-blower - means the person that reports a Concern committed in a work-related context outside the normal management reporting channels.

Whistle-blowing means the reporting of a Concern committed in a work-related context outside the normal management reporting channels.

4 Standards, KPIs and KRIs

Standards

Reporting

4.1 All Employees and Third Parties are encouraged to report Concerns and should feel no restraint in doing so.

4.2 The Whistle-blower is not responsible for investigating Concerns or for determining fault or corrective measures; appropriate management officials are charged with these responsibilities.

4.3 Employees and Third Parties must follow the Whistle-blower Procedure when reporting a Concern.

No retaliation

4.4 No Employee, Third Party or other person (as defined below) who reports a Concern whilst acting in good faith shall be subject to retaliation or, in the case of an Employee, to adverse employment consequences. Other persons (besides the Employee or Third Party) include:

(a) facilitators;

(b) third persons who are connected with the Whistle-blower and who could suffer retaliation in a work-related context, such as colleagues or relatives or the Whistle-blower; and

(c) legal entities that the Whistle-blower owns, works for or is otherwise connected with in a work-related context.

4.5 Moreover, Employees who retaliate against a Whistle-blower will be subject to disciplinary measures including but not limited to dismissal and administrative sanctions.

Acting in good faith

4.6 The Whistle-blower must act in good faith and must have reasonable grounds for a Concern. The act of reporting a Concern that proves to be unsubstantiated, malicious, reckless, or with the foreknowledge that the allegations made in the report are false, will be viewed as a serious disciplinary offence and may result in disciplinary measures including but not limited to dismissal and administrative sanctions.

Confidentiality

4.7 Reports of Concerns, and investigations pertaining to these, must, as far as possible, be treated as confidential. The identity or any information relating to the Employee or Third Party shall not be disclosed to anyone beyond authorised employees without their explicit consent.

4.8 Disclosure of reports of Concerns to individuals without a need to know will be viewed as a serious disciplinary offence and may result in disciplinary measures including but not limited to dismissal and administrative sanctions. Such conduct may also give rise to other actions, including civil lawsuits.

4.9 Whistle-blowers raising a Concern whose own conduct is implicated in the Concern will not be given any automatic immunity from investigation, disciplinary action, criminal prosecution and/or civil liability. The same applies to any other Employee or Third Party that provides information, causes information to be provided, or who otherwise assists an investigation.

Policy deviations

4.10 Any specific deviation from this Policy must be subject to prior approval by the Head of Internal Audit.

KPIs and KRIs

4.11 None.

5 Roles and responsibilities

First line and second line responsibilities

5.1 **Executive Committee** - the Intertrust Group Executive Committee (**Exco**) is the required approval body for material changes to this Policy (with minor changes to be approved by the Chief Financial Officer) and is ultimately responsible for setting the tone and culture of Intertrust Group at a global level to facilitate the proper operation of this Policy.

5.2 **Local Management -** Local Management (Managing Directors, Service Line Directors and Directors of central functions (eg Finance, HR, Operations)) is responsible for: (i) making sure that the all associated laws and/or regulations associated with this Policy are complied with in full at the local level; and (ii) setting the tone and culture of Intertrust Group at a local level to facilitate the proper operation of this Policy.

Third line responsibilities

5.3 **Internal Audit** - Internal Audit is responsible for:

(a) review of the Policy every three years at minimum or when major changes have taken place. The Head of Internal Audit is responsible for the timely maintenance of this Policy;

(b) providing Exco with management information sufficient to facilitate assessment of the ongoing adherence to and operation of this Policy by the business; and

(c) considering the independent third line of defence oversight of implementation of this Policy in each of the Intertrust Group offices.

6 Policy adherence - consequence management

6.1 Not complying with this Policy may result in internal and/or external disciplinary measures including but not limited to financial penalties such as withholding of bonus or salary increases, dismissal, administrative and/or criminal sanctions.

7 Implementation and training

7.1 The Head of Internal Audit is responsible for the implementation of changes to this Policy globally.

7.2 Local Management is responsible for the implementation of changes to this Policy at the local level, which must be completed within three months of the date of its publication.

7.3 The relevant Global Function Head is responsible for implementation of this Policy in their functional area (to the extent that it is applicable) and this must be completed within three months of the date of its publication.

7.4 Central GRC will communicate this Policy to all employees either via Intertrust Group's intranet site or in another manner. Central GRC will also publish a Bridge news article with notification of the changes to be available to the Business.

7.5 This Policy will also be published on the Intertrust Group website.

8 Further guidance and supporting information

8.1 Records of every report shall be stored as long as it is necessary, and Whistle-blowers shall be offered the opportunity to check these records.

8.2 Any processing of personal data must be carried out in accordance with the Data Processing Protocol published on our website. This includes that personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

Whistle-blower - Global Procedure

This Procedure must be read and understood in conjunction with the Whistle-blower Policy. All capitalised terms, not otherwise defined herein, have the same meaning as in the Policy.

1 All Employees

Steps to be completed by the Whistle-blower:

Reporting of Concerns

1.1 Discuss your Concern with your immediate manager (or other management representative). You should proceed with making a Whistle-blower report to the Group Head of Internal Audit:

(a) if your Concern is not resolved to your satisfaction; or

(b) if you are uncomfortable speaking with your manager, or the manager is a subject of the Concern.

Who to inform, how to report

1.2 You can make your report in one of the following ways:

(a) verbally to the Head of Internal Audit (this must be followed by an email submission, see (b) below);

(b) by email to: whistleblowing@intertrustgroup.com (Note: the Head of Internal Audit has sole access to this e-mail account);

(c) anonymously by letter to the Head of Internal Audit:

(i) mark as 'confidential - to be opened by the addressee only' and send to: *Head of Internal Audit, Intertrust Group, Basisweg 10, 1043 AP Amsterdam*;

(d) by letter (anonymously or otherwise) to the Chair of the Supervisory Board of Intertrust N.V. (**Supervisory Board**):

(i) only use this method to report a Concern relating to the functioning of a member of the management board of Intertrust N.V. (**Management Board**) or the Head of Internal Audit;

(ii) mark as 'confidential - to be opened by the addressee only' and send to: *Chair of the Supervisory Board, Intertrust N.V., Basisweg 10, 1043 AP Amsterdam*.

1.3 You must include all the information you have about your Concern and any related event(s), such as:

(a) the date of the event(s);

(b) the nature of the event(s);

(c) the name of the person(s) involved in the events;

(d) (possible) witnesses to the event(s); and

(e) evidence of the event(s), eg documents, e-mails or file notes.

1.4 You must respond to any reasonable request to clarify any facts and/or circumstances, provide (additional) information and cooperate with any investigation into the Concern(s) by the Head of Internal Audit/Chair of the Supervisory Board. A lack of information can be the reason for deciding not to conduct an investigation into your Concern and/or to conclude that this has no factual basis.

Unless you made your report anonymously, you should be contacted to confirm the ultimate outcome of any assessment and investigation in respect of your Concern.

2 Head of Internal Audit/Chair of the Supervisory Board (Investigator)

Steps to be completed by the person receiving a Whistle-blowing report:

Handling of reported violations

2.1 On receipt of a written Concern, immediately notify the Head of Internal Audit or the Chair of the Supervisory Board (as relevant), the Chair of the Risk Committee of the Supervisory Board and the members of the Management Board:

(a) Exception: any person that is the subject of the Concern.

2.2 Agree who will complete the required steps below:

(a) The presumption is that this will be the Head of Internal Audit unless he/she is the subject of the Concern.

2.3 Notify the Whistle-blower and acknowledge receipt of the report relating to the Concern within seven business days:

(a) Exceptions: (i) where the submission has been made anonymously; and (ii) subject to leave from the office.

2.4 Assess and investigate the Concern (ie, evaluate and recommend closure, or evaluate and recommend investigation) under the direction of the Chair of the Risk Committee:

(a) The Head of Internal Audit, the Risk Committee and/or a member of the Management Board may retain legal advisers, accountants, or external investigators to conduct a full and complete investigation of the Concern(s).

2.5 On completion of the investigation, prepare a report (and/or obtain this from the external party engaged) setting out recommendations for appropriate corrective actions to the Chair of the Supervisory Board, the Chair of the Risk Committee, and the members of the Management Board.

(a) Corrective actions identified should include providing feedback to the Whistle-blower (if not anonymous) on the outcome of their report and a follow-up on corrective action(s) taken by management.

(b) The feedback must be provided within a reasonable timeframe, not exceeding three months from the date of the acknowledgement of receipt.