

Hitachi Group Whistleblowing Policy

Owner: Compliance Department, Compliance Division

Publication Date:

Effective Date:

Applicability: Global

Introduction

Hitachi, Ltd., together with its group companies, subsidiaries, and affiliates (collectively, Hitachi), maintains a culture of openness and is committed to the highest standards of sincerity, accountability, and ethical conduct.

An essential characteristic of our open culture is the availability of appropriate channels for Hitachi employees and other stakeholders to report concerns in good faith and the ability to do so without fear of reprisal.

Hitachi Group Code of Ethics and Business Conduct identifies various channels to report a concern. These channels include managers, Human Resources, Legal, Ethics & Compliance departments, and the Hitachi Global Compliance Hotline (thereafter referred to as hotline). Hitachi employees and other stakeholders can report a concern anonymously, where permitted by law, through the hotline if they wish to do so.

It is the responsibility of every Hitachi employee to speak up and report misconduct when they see it. Managers have a responsibility to listen to concerns and respond appropriately.

The Global Compliance Office is accountable for the oversight and management of the hotline and concerns management process.

1. Scope and exclusion

This policy applies to:

- all current and former Hitachi employees (whether full-time or part-time);
- those belonging or once belonged to administrative, management or supervisory boards of Hitachi;
- those who supply/supplied goods or services to Hitachi, including secondees, external consultants, contractors (extended workforce) or to those working under the supervision of such persons;
- agency personnel;
- customer executing sales contract with Hitachi;
- those who acquire information during a recruitment process or pre-contractual discussions with Hitachi;
- shareholders of Hitachi; and
- civil servants;

who are seeking to report a concern about actual or suspected misconduct (in the European Union (EU), such concerns will include the Relevant Concerns listed in Annex 1, and all such individuals are referred to collectively as Relevant Individuals).

This policy also applies to third persons with a connection to the persons mentioned above (such as their colleagues or relatives, persons providing them with assistance, or legal entities connected to them).

This policy does not govern employee grievances, complaints relating to job performance, or the terms and conditions of employment, which are not by their nature complaints which relate to a potential malpractice / material misconduct.

If this policy indicates a requirement that is less restrictive than the local regulatory requirements or in conflict with the local law, the applicable regulatory requirement must be followed, and Hitachi, Ltd.'s Chief Compliance Officer shall be notified. Any deviation from this policy shall be requested in writing from Hitachi, Ltd.'s Chief Compliance Officer.

This policy may be amended from time to time and may be supplemented with additional local measures to account for local law or local regulatory requirements.

2. Terms and definitions

The following terms and definitions in this policy align with International Organization for Standardization standards.

- **Shall** indicates a requirement per Hitachi policies and procedures.
- **Should** indicates a recommendation.
- **May** indicates a permissive statement and an option that is neither mandatory nor specifically recommended.

3. Policy requirements

3.1. Reporting a concern

3.1.1. The availability of various speak-up channels within Hitachi (managers, Human Resources, Ethics and Compliance and Legal departments, and the hotline) allows people to choose the channel most suitable to their circumstances. Concerns can be reported in writing or orally, including through face-to-face meetings, upon request by the reporting person, or through the hotline (telephone or online). NAVEX, an independent third party receives, and processes reports in a secure and confidential manner. The hotline is available 24/7 and allows a person to remain anonymous, where permitted by law. Where a person requests a face-to-face meeting, the meeting shall be arranged to take place as soon as reasonably possible.

3.1.2. While Hitachi would like employees to feel comfortable speaking up internally and allow the company the chance to deal with the issue, nothing in this policy prohibits employees from reporting possible violations of laws or regulations including but not limited to any relevant government agency or entity for the concerned jurisdiction, which may be appropriate in certain circumstances.

3.1.3. Any concern reported by a person shall be taken seriously and addressed appropriately, promptly, and (as far as is possible in the circumstances) confidentially, with appropriate feedback provided to the person.

3.2. Evaluation of concerns

3.2.1. Concerns shall be evaluated promptly and effectively to determine the appropriate course of action. Such evaluation should be completed within three business days of receiving the concern, but no later than seven calendar days.

3.2.2. Evaluation of material misconduct shall include consultation with the Hitachi, Ltd.'s Chief Compliance Officer or their delegate, each business unit's or group company's head of compliance or their delegate, Human Resources or Legal as appropriate.

3.2.3. Persons designated to receive and/or investigate concerns shall have the competency, capacity, and appropriate authority to manage and follow up on the reports. These persons shall be independent and abstain from the case if they have any conflicts of interest related to the case and report the conflict of interest according to the Conflicts of Interest protocols.

3.2.4. Persons shall be notified of the receipt of the concern promptly and in any event within seven business days of raising it. Appropriate lines of communication shall be maintained with the person, and further information may be sought from them as required.

3.2.5. Hitachi, Ltd.'s Chief Compliance Officer or each business unit's and/or group company's head of the compliance shall be notified of any material misconduct including where a concern becomes material misconduct during the investigation.

3.3. Protection

Hitachi has a zero tolerance policy for retaliation of any kind against persons who report concerns.

3.3.1. This policy is designed to offer protection to persons who had reasonable grounds to believe that a concern had arisen at the time of reporting.

3.3.2. Protection is available to persons reporting a concern anonymously if the conditions of this policy are met.

3.3.3. Protection shall be provided against all forms of actual, threatened or attempted retaliatory measures (in the EU, these will include the specific measures listed in **Annex 1**). Persons can also consult a legal advisor to obtain advice on the procedures and remedies available to them, their protection against retaliation and their rights as a whistleblower.

3.3.4. Protection cannot apply to those who report information already fully available in the public domain or unsubstantiated rumors and hearsay where they do not have a reasonable belief in a possible concern.

3.3.5. Except for cases where identifying the person who reported the concern is essential to conduct the investigation, Hitachi officers/employees shall not attempt to identify the reporter and those supporting the investigation.

3.3.6. Any act of retaliation shall be treated by Hitachi as a violation of its applicable rules and policy and could result in disciplinary action up to and including dismissal.

3.3.7. Disciplinary action may be taken by the company against any employee deliberately raising false and malicious allegations or otherwise acting in bad faith.

3.4. Confidentiality

3.4.1. Strict confidentiality shall be applied, to the extent possible, to handling concerns, including investigation details and the identity of the person making the allegation.

3.4.2. Hitachi shall take all reasonable steps to maintain confidentiality as far as possible during and after the reporting and investigations processes to ensure that the person making the report, the reported concern, or any other persons or items mentioned in the report are not improperly disclosed to non-authorized persons.

3.5. Investigation

3.5.1. Hitachi is committed to following up appropriately, promptly, and (as far as is possible in the circumstances) confidentially, with appropriate feedback provided to the person on concerns raised.

3.5.2. Hitachi officers/employees are required to cooperate with investigations conducted in accordance with this policy.

3.5.3. The forms of malpractice/ material misconduct which could warrant an investigation and might require formal disciplinary action (including termination of contract or dismissal in the most serious cases) include but are not limited to:

- a) Breach of Hitachi's internal policies and Hitachi Group Code of Ethics and Business Conduct
- b) Fraud or corruption, including bribery
- c) Irregularities involving accounting or other financial procedures
- d) Commission of any criminal offense
- e) Conduct which is, or may be, in conflict with Hitachi's interests, for example, inappropriate contacts with a business competitor
- f) Dishonesty or other irregularities in dealing with customers and suppliers
- g) Conduct that endangers the health and safety of the public, employees and other Hitachi workers and visitors
- h) Failure to comply with a legal obligation
- i) Environmental damage arising from Hitachi's activities or those of its employees or workers on Hitachi business
- j) Discrimination, bullying and harassment
- k) Act or omission resulting in damage or risk of harm to human rights or the environment
- l) Breach of any other legal or regulatory requirement

3.5.4. Chief Compliance Officer (each group company's) or each company's head of compliance shall appoint an investigator who will take responsibility for the investigation, including notifying the investigator of the confidential obligations they would be bound to. The criteria for selecting an investigator and the way of appointment (by email or in writing) are outlined in the Concerns Management policy.

3.6. Response and timescale

3.6.1. it is imperative that the person making the report is informed of the investigation progress and outcome within a reasonable timeframe -- not exceeding three months -- and as much as legally possible without breaching confidentiality to build and maintain trust in the effectiveness of the concerns management process, including whistleblower protection. In complex cases where this timeframe could be longer, the person should be informed within a reasonable timeframe and given an expected completion date for the investigation. Even where Hitachi might be constrained by confidentiality, it shall still try to provide the reporter with as much information as possible about the steps that have been taken in response to their concerns.

3.6.2. When reporting a concern via the hotline (telephone or internet), persons must select options that correctly correspond to their disclosure. Accordingly, the report is received and processed by NAVEX in a secure and confidential manner in compliance with European data protection legislation. NAVEX forwards the report to the designated person in the relevant business to process.

3.6.3. After the report is submitted via the hotline, the person making the report is given a PIN (Personal Identification Number) to use online to follow the progress of their report and respond to any questions from the investigator. Adequate information on the case is necessary to launch and complete the investigation. Hence, it is imperative for the person to periodically check and respond any outstanding questions from the investigator.

Annex 1 - EU Annexure

Definitions:

- A *relevant concern* refers to possible breaches of EU law in the areas listed in Article 2(1) of Directive (EU) 2019/1937, including: (a) public procurement; (b) financial services, products and markets, and prevention of money laundering and terrorist financing; (c) product safety and compliance; (d) transport safety; (e) protection of the environment; (f) radiation protection and nuclear safety; (g) food and feed safety, animal health and welfare; (h) public health; (i) consumer protection; (j) protection of privacy and personal data, and security of network and information systems; (k) breaches affecting the financial interests of the European Union as referred to in Article 325 Treaty on the Functioning of the European Union (TFEU) and as further specified in relevant European Union measures; and (l) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of European Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.
- For the purposes of Section 3.3.3, such retaliatory measures shall include, but not be limited to, the following: (a) suspension, lay-off, dismissal or equivalent measures; (b) demotion or withholding of promotion; (c) transfer of duties, change of location of place of work, reduction in wages, change in working hours; (d) withholding of training; (e) a negative performance assessment or employment reference; (f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty; (g) coercion, intimidation, harassment or ostracism; (h) discrimination, disadvantageous or unfair treatment; (i) failure to convert a temporary employment contract into a permanent one, where the Relevant Individual had legitimate expectations that they would be offered permanent employment; (j) failure to renew, or early termination of, a temporary employment contract; (k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income; (l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the Relevant Individual will not, in the future, find employment in the sector or industry; (m) early termination or cancellation of a contract for goods or services; (n) cancellation of a license or permit; (o) psychiatric or medical referrals.