VenHub Global, Inc.
Whistleblower Policy

I. Overview and Purpose

This policy establishes guidelines and procedures for handling whistleblower claims within VenHub, its wholly owned subsidiaries, and any affiliated entities over which VenHub exercises control. It ensures a fair response to allegations by employees, suppliers, customers, or contractors, protecting those who step forward in good faith from retaliation and providing targets of allegations an opportunity to present relevant evidence and understand the nature of the allegations.

The policy details the actions required by:

1. **Individuals** who have knowledge of any facts or indications of serious breaches of policy or the law.
2. **Company Management** when whistleblower allegations are made.

II. Scope

This policy applies to all VenHub employees and subsidiaries worldwide. It governs procedures that must be followed when allegations of impropriety or irregularity are made by a whistleblower, specifically when such allegations are:

1. Relate to accounting, internal accounting controls, or auditing matters;
2. Could cause serious damage to the company's brand or reputation; or
3. Could result in material liability to the Company.

Allegations outside the scope of this policy should be referred to the General Counsel's Office (GCO) for appropriate action.

III. Key Definitions

1. **Whistleblower:** An individual who, in good faith, reports or discloses information about suspected wrongdoing, impropriety, or non-compliance with laws, regulations, company policies, or ethical standards, regardless of whether the matter has been previously reported through other channels.

2. **Target**: The person potentially implicated in the whistleblower allegations.

IV. Roles & Responsibilities

1. **Manager Responsibilities:** Managers at all levels are responsible for upholding integrity and ethical standards. Upon learning of any allegations, managers must contact the GCO immediately to initiate an appropriate investigation.

2. **Employee Responsibilities**: Employees who suspect serious breaches of policy or law are expected to report them promptly to their leaders. If it is impractical or inappropriate to notify an immediate supervisor, employees may contact management via email at whistleblower@venhub.com. Employees should provide objective evidence to support their allegations and retain all documents relevant to the investigation.

V. Policy Requirements

1. **Allegations That May Form Whistleblower Claims**: The following is an indicative list of the types of allegations that may form whistleblower claims within the scope of this policy. This list is not exhaustive:

    i. Internal business practices inconsistent with GAAP.
    ii. Falsification, alteration, or substitution of company records.
    iii. Violations of the Company Code of Conduct, including:
        1. Conflicts of interest.
        2. Inaccuracies in books and records.
        3. Insider trading.
        4. Collusion with competitors.
        5. Money laundering.
        6. Data protection infringements.
        7. Corruption and bribery.
    iv. Authorizing, directing, or participating in significant ethical violations.
    v. Deliberately concealing or withholding information about significant ethical violations.
2. **Investigating Whistleblower Claims:** The Audit Committee Chairman (or representative) is responsible for directing all aspects of investigations, including the assignment of internal or external personnel as needed. Investigations should be conducted confidentially, safeguarding against unfounded or inaccurate accusations. The target of any allegations will have the opportunity to present relevant evidence and understand the nature of the allegations.

3. **Data Privacy and Confidentiality:** All personal data gathered during investigations will be handled in accordance with local data privacy laws, including GDPR and other applicable regulations. The company will implement specific technical and organizational measures to ensure data security, including encryption, access controls, and data minimization principles. A detailed data retention schedule will be maintained specifying the retention periods for different categories of investigation-related data. Information will be kept secure and only accessible to those who need to know to perform their job duties. Data identifying the whistleblower, or the target will not be retained longer than necessary to satisfy legal obligations.

4. **Disciplinary Measures:** Decisions on disciplinary actions based on investigation findings must be approved by the Audit Committee Chairman. Disciplinary

measures will be applied in consultation with Human Resources, considering the intent and cooperation of the target.

5. **Prohibition of Retaliation:** No adverse action of any kind, including but not limited to discrimination, harassment, threats, demotion, salary reduction, or termination may be taken against a whistleblower in retaliation for reporting allegations in good faith. Any person found to have engaged in retaliatory conduct will be subject to immediate disciplinary action, up to and including termination. Allegations not made in good faith are a misuse of the whistleblower process and may result in disciplinary action against the whistleblower.

VI. Compliance with Nasdaq Requirements: VenHub is committed to complying with all Nasdaq requirements regarding whistleblower policies, ensuring:

1. **Confidentiality and Anonymity**: Whistleblowers can report anonymously where permitted by law, and their identity will be protected.
2. **Fair Treatment**: The policy ensures fair treatment for both the whistleblower and the target, adhering to due process standards.
3. **Training and Awareness**: Regular training will be provided to all employees and management to ensure awareness and understanding of this policy.
4. **Oversight and Accountability**: The Audit Committee Chairman is responsible for overseeing the implementation and adherence to this policy, ensuring timely and thorough investigations.

VII. Policy Review and Updates: This policy will be reviewed annually by the Audit Committee to ensure compliance with applicable laws and Nasdaq requirements. Updates will be made as necessary to address changes in laws, regulations, or company practices.