

# **The United Laboratories Anti-Fraud and Whistleblowing Management Policy**

## **1. Purpose**

The United Laboratories International Holdings Limited (Stock Code: 3933.HK) (“TUL”, the “Group”, “we”) has established this policy to protect the interests of the Group, prevent fraudulent behavior, standardize the management of whistleblower reports, and reduce operational risks.

## **2. Definition of Fraud**

For the purposes of this policy, fraud refers to actions carried out by internal or external personnel through deception or other illegal or non-compliant means to obtain improper personal benefits. These include, but are not limited to, the followings:

- (1) Illegal use, embezzlement, misappropriation, theft, occupation, or trade of the Group’s assets;
- (2) Abuse of authority by management personnel to engage in illegal or non-compliant economic activities;
- (3) Falsifying, misreporting, concealing, or altering accounting records, information documents, or business transactions;
- (4) Disclosing the Group’s trade secrets or violating non-compete agreements;
- (5) Forging, misusing, or stealing official company seals;
- (6) Other acts involving commercial bribery, such as bribery or acceptance of bribes;
- (7) Any other behavior that damages the Group’s economic interests or seeks improper personal gain.

## **3. Scope of Application**

The following behaviors are considered violations under this policy:

- (1) Employees using their position to embezzle, steal, defraud, or otherwise unlawfully appropriate the Group’s assets, such as falsifying expenses, misappropriating company funds;

- (2) Accepting or soliciting any benefits or benefit transfers from suppliers or other partners, such as cash, securities, gift cards, payment vouchers, or expense reimbursements;
- (3) The employee, their spouse, children, or other relatives accepting any benefits or favorable conditions from suppliers or partners;
- (4) Investing in or establishing competing businesses in the name of the employee or their spouse;
- (5) Using the Group's business channels, intellectual property, or other resources for personal or third-party gain or benefit transfers;
- (6) Using Group assets under a personal or third-party name to register companies, invest in shares, purchase stocks, real estate, or engage in other commercial activities in China or abroad (unless approved by the Board of Directors);
- (7) Abusing authority to engage in illegal or non-compliant business activities, or directing/coercing others to violate laws or company policies;
- (8) Falsifying, misreporting, concealing, or altering accounting records, information documents, or business transactions;
- (9) Disclosing the Group's trade secrets or violating non-compete obligations;
- (10) Forging, misusing, or stealing company seals;
- (11) Any other acts of commercial bribery, including giving or accepting bribes;
- (12) Any other behavior that harms the Group's economic interests or seeks improper personal gain.

#### **4. Rights and Obligations of Whistleblowers**

Whistleblowers must comply with the following regulations:

- (1) Abide by all applicable laws, regulations, and the Group's internal policies;
- (2) Provide the name of the person being reported, along with specific facts and evidence of the alleged violations, and bear responsibility for the truthfulness of the report;
- (3) Refrain from engaging in illegal or criminal activities under the guise of whistleblowing;

(4) Report through official channels designated by the Group, including published hotlines, email addresses, or whistleblowing websites;

(5) Cooperate actively in investigations when required and must not provide false information or obstruct the investigation process.

## **5. Rights and Obligations of Personnel Handling Whistleblower Reports**

Personnel responsible for receiving and handling whistleblower reports must adhere to the following work principles:

(1) Face-to-face reports must be received in a confidential setting, with designated staff conducting the discussion. Unrelated personnel may not be present, inquire, or take notes;

(2) All activities related to the handling of whistleblower letters—receiving, opening, logging, transferring, storing—as well as the reception, recording, and audio logging of phone reports, must strictly follow confidentiality principles;

(3) The identity of the whistleblower must be kept strictly confidential. Under no circumstances may the complaint materials be shown to the accused or any unrelated party, nor may the case details be disclosed or discussed;

(4) It is strictly forbidden to excerpt, copy, withhold, hide, or destroy whistleblower materials without authorization;

(5) Whistleblowers must not be harassed or threatened;

(6) Whistleblowing matters must be managed by dedicated personnel and handled through dedicated processes;

(7) Any personnel found to have violated the above regulations will be held accountable by the Group. If a criminal offense is involved, the matter will be referred to judicial authorities;

(8) Upon conclusion of an investigation, investigators should provide appropriate feedback to the whistleblower, based on the method of reporting;

(9) No department or individual within the Group may interfere with or obstruct the investigation or resolution of whistleblower matters.

## **6. Handling of Fraud**

The Group's Supervision Department is responsible for overseeing the Group's anti-fraud efforts. This includes organizing fraud risk assessments, establishing and

maintaining whistleblower channels and procedures, receiving and investigating fraud cases, and issuing fraud evaluation and resolution reports.

Upon receiving reports or leads related to potential fraud, investigators must promptly analyze and assess the information. If the initial investigation indicates that the allegations are likely valid, a formal investigation plan should be developed and the matter handled according to the following principles:

- (1) In general, for cases involving ordinary employees, the matter should be reported to the general manager or relevant leader of the business unit after preliminary evaluation, and an official investigation should be initiated.
- (2) For cases involving mid-level managers (including those of holding subsidiaries), senior executives, or other significant fraud incidents, the matter must be escalated to the Board of Directors for resolution after preliminary evaluation.
- (3) If the accused is a member of the investigation team, the case must be referred to senior Group leadership for handling.
- (4) In special circumstances, investigators may, with approval from the relevant management level, exercise independent investigation authority directly.
- (5) Disciplinary violations by other personnel will be handled in accordance with the Group's established disciplinary procedures.
- (6) With appropriate approval, the Group's Supervision Department may independently decide the composition of the investigation team, the scope, timeframe, and methods used. All other departments and individuals must cooperate fully and must not obstruct the investigation.
- (7) Based on investigative needs, investigators have the right to request relevant documents and records from the accused department or individuals, including accounting vouchers, financial statements, etc. Personnel involved may be required to provide explanations or clarifications, and must fully cooperate.
- (8) Employees found to have engaged in fraudulent behavior will be dealt with by the relevant department according to internal disciplinary procedures based on the investigation results and recommendations. If the behavior constitutes a criminal offense, the case will be transferred to judicial authorities for legal processing.
- (9) If the investigation concludes that the whistleblower's incorrect report was due to incomplete understanding of the facts and not malicious intent or defamation, no accountability will be pursued.

(10) If it is determined that the complaint was maliciously fabricated or defamatory, appropriate disciplinary action or recommendations will be made based on the severity of the harm caused to the accused or to the Group.

(11) After the investigation is completed, investigators must issue a final report including findings, disciplinary recommendations, corrective measures, and internal control assessment. These should be submitted to the Group's management and Board of Directors, and the case documentation should be properly archived in accordance with the Group's record-keeping policies.

## **7. Protection and Reward Measures for Whistleblowers**

No individual is permitted, under any pretext, to retaliate against whistleblowers. Retaliation includes condoning, covering up, bribing, or instigating others to infringe upon the legitimate rights and interests, such as personal safety or property of the whistleblower or their family members. The Group will hold individuals engaging in retaliatory acts accountable. If the act constitutes a crime, it will be referred to judicial authorities. Whistleblowers have the right to demand that the retaliators cease the infringement, issue an apology, and compensate for any losses. They may also file a lawsuit directly with the court.

If a whistleblower faces retaliation, they may report it to the responsible department or higher authorities. If the whistleblower's personal safety is threatened, relevant departments must take immediate protective measures and, if necessary, coordinate with external authorities.

If a whistleblower suffers unjust treatment due to their report, the Group's Supervision Department shall recommend corrective action to the responsible or supervisory unit upon verification of the facts.

If a report is verified to be true and helps the Group recover losses, the whistleblower may be commended or rewarded according to the following guidelines:

(1) In principle, rewards are limited to whistleblowers who report under their real names. If an anonymous report leads to the successful resolution of a case and the whistleblower's identity can be confirmed, a reward may be issued according to regulations;

(2) If the same issue is reported by multiple individuals independently, only the first reporter will be rewarded. If a report is made jointly by two or more individuals, it will be treated as one case and rewarded accordingly;

(3) Rewards are proposed by the investigators after case closure and issued upon approval from Group leadership;

(4) Whistleblowers must claim their reward within one month of receiving the notice. Failure to do so will be considered a waiver of the reward;

(5) Anyone found to have violated this policy, disclosed whistleblower information, or fraudulently obtained reward money will be dealt with in accordance with disciplinary rules. If the offense constitutes a crime, it will be referred to judicial authorities for criminal prosecution;

(6) When publicizing or recognizing outstanding whistleblowers, no personal information—such as name, contact details, or any identifying data—may be disclosed without the whistleblower’s explicit consent.

## **8. Fraud Penalty Policy**

Once a report involving an employee is verified, the Group will immediately terminate the employment relationship with the individual involved and reserves the right to pursue criminal charges and other legal responsibilities in accordance with the law.

The Group has established a blacklist system. If a report against a supplier or business partner is confirmed to be true, the entity will be placed on the blacklist and all future cooperation will be terminated.

## **9. Supervision of Anti-Fraud Efforts**

The Board of Directors is responsible for overseeing and guiding the Group’s anti-fraud work. The Group’s Supervision Department will report to the Board on a regular basis regarding the anti-fraud work plan, its implementation, the status of fraud-related complaints and investigations, findings, and recommendations. The Center will also follow the Board’s instructions and maintain proper written documentation for future reference.

When formulating and executing the annual supervision and reporting plan, the Group’s Supervision Department must consider the identification and evaluation of fraud risks and provide guidance for implementing the Group’s anti-fraud initiatives.

## **10. Fraud Prevention**

All levels of management within the Group must, within their areas of authority, promote the corporate culture of “friendly, responsible, hardworking and highly efficient”, advocate a “fair, just and transparent” team environment, and maintain a sound internal control system. This includes, but is not limited to:

(1) Leading by example and strictly complying with the Group’s rules and policies;

(2) Organizing risk assessments, internal control activities, and anti-fraud training programs;

- (3) Encouraging employees to act lawfully and with integrity;
- (4) Establishing and implementing effective reward and punishment policies.

In high-risk areas and key positions, responsible personnel must implement segregation of duties and corresponding control measures. These may include signing self-discipline agreements, establishing registration and handover systems, providing anti-fraud and ethics training, and incorporating fraud risk control into their core job responsibilities.

Personnel directly involved in anti-fraud work should continuously enhance their awareness and technical capabilities, stay informed about the Group's operational developments and plans, and build relationships with external agencies for regular communication and information exchange.

## **11. Supplementary Provisions**

This policy was issued by the Group's Audit and Legal Affairs Centre and came into effect on November 1, 2018. It was subsequently revised by the Group's Supervision Department and reissued on April 21, 2025, with immediate effect.