



## Summary of the Whistleblowing Policy – Incident Reporting



01/05/2023



## Summary of the Whistleblowing Policy – Incident Reporting

### Scope and basic principles of the Policy

The Whistleblowing Policy – Incident Reporting (hereinafter referred to as the "Policy") sets out the principles and operating framework under which the Company (hereinafter referred to as Quest Holdings) and Group members receive, process and investigate signed and anonymous reports/incidents of irregularities, omissions or other criminal acts brought to the attention of staff or other third parties (e.g., customers, suppliers).

### Personal Scope

The incident reporting procedure applies to: (a) members of the Board of Directors and persons performing managerial functions in Group members, (b) Group personnel, and (c) any third party (e.g., customers, suppliers, person providing services to Group members) who possesses evidence and/or information about irregular or illegal actions (already committed or about to be committed) concerning the Company or Group members.

### Material Scope (scope of reports/incidents)

Reports are made on the basis of a sincere and reasonable belief that a criminal act or misconduct has been committed or is likely to be committed. Employees or third parties (customers, suppliers, etc.), of the Company and Group members are encouraged to report criminal acts, suspected incidents of illegal conduct, incidents of mismanagement or serious irregularities-omissions in relation to the Regulations, Policies and Procedures of the Company and Group members.

In particular:

Reports/incidents of irregularities, omissions or criminal acts relate to - but are not limited to - the following:

- Theft
- Fraud.
- Corruption
- Bribery (offer/receipt)
- Violation of human rights (diversity, discrimination based on gender, religion, nationality, etc.)
- Abuse of assets
- Acts that endanger the health and safety of workers
- Acts harmful to the environment
- Acts that may lead to a breach of free competition law
- Acts which conflict with the interests of the Company and/or the Group
- Violation of the Policies and Procedures of the Company and Group members with a risk of causing financial damage
- Violation of the legal framework governing the Company and its Group members (including the legislation governing the protection of persons reporting violations of EU law)
- Other unethical/improper conduct (acts that violate the Group's Code of Conduct and Ethical Behavior rules).

The above list is not exhaustive, but is intended to illustrate indicatively the type of issues that fall within the scope of this Policy.

A person making a report need not have a high degree of certainty or proof; the expression of an honest suspicion will be sufficient if s/he had reasonable grounds to believe that the report was necessary to disclose the violation.

The scope of this Policy **does not cover**:

- incidents of violence and harassment
- data breaches
- security incidents

In the above cases, the provisions of the relevant Policies and Procedures of the Company and Group members are followed.

### **Anonymity of the Reporting Person**

The Company and Group members encourage anonymous incident reporting and guarantee that all messages received will be treated confidentially.

If the reporting person does not wish to submit a message by name, s/he has the option to submit the report anonymously.

### **Protection of the reporting person and the person concerned**

Reports/ must be made in good faith. The Company and Group members are committed to protect stakeholders who have made a report in good faith, without abusing the report management mechanism, or participated in the investigation of a potential violation, by:

- (a) any acts of retaliation (reduction in salary or leave, change in working hours, exclusion from work matters, transfer, change in scope of work, termination of cooperation, etc.),
- (b) any other kind of discrimination or any kind of unfavourable treatment.

### **Incident reporting channels**

Any employee or third party (e.g., partner/supplier) may submit a report in writing (signed or anonymously) in the following ways:

- By e-mail to:  
milisemas@company.gr (where company fill out the respective Quest Group member),  
In the case of an anonymous report: it is recommended to use a non-corporate email to submit the report (e.g., gmail)
- By post to the address of the respective Quest Group member to the attention of the Compliance Officer.

### **Receiving & Monitoring Reports Officer (RMRO)**

The person responsible for receiving and monitoring reports is the Compliance Officer of the Company or the Compliance Officer of each key Group subsidiary, depending on the company to which the report/incident relates. Moreover, the report/incident shall only be communicated for information to the Human Resources Officer of the company to which the report/incident relates.

### **Duties of the Receiving & Monitoring Reports Officer**

The RMRO must:

- carry out his/her duties with integrity, objectivity, impartiality, transparency and social responsibility,
- respect and observe the rules of confidentiality and secrecy on matters of which s/he has become aware in the performance of his/her duties,
- abstain from managing specific cases, declaring that s/he is prevented from acting, where there is a conflict of interest.

### **Record keeping**

The RMRO of the Company or the Group member shall keep a file, either in electronic form or hard copy, which contains at least the following information for each report/incident:

- number, subject, category and origin,
- information on the investigation of each report and the documents relating to it,
- the final outcome of the investigation and the action taken.

### **Personal Data**

Any processing of personal data under this Policy shall be carried out in accordance with the relevant national and EU legislation. The data of all parties involved are protected and processed for the sole purpose of verifying the validity of the specific report and investigating the specific incident.

**Approval and revision of the Policy** This Policy is approved by the Board of Directors of the Company and the Group members, is reviewed annually and revised whenever necessary.