Scope of services: RETEMS Logistics is a provider of International Freight Forwarding, Warehousing and Customs Clearance Services.
This policy applies to all workers and includes employees and contingent workers, non-RETEMS Logistics workers including contractors, joint ventures, third parties, or other agents (hereafter referred to as "User") engaged by RETEMS Logistics worldwide. Where these standards are not followed, this should be highlighted to the Director, Line Manager.

Statement: The purpose of this policy is to outline an effective information security and risk management framework that combines administrative, physical, and technical controls to protect the confidentiality, integrity, and availability of RETEMS Logistics information and assets. It provides the baseline for a robust security culture, setting rules for expected behaviours and defining steps required to monitor, investigate, and minimize information security risk to RETEMS Logistics.

Definitions:

- **Information Assets** - Any information that is essential RETEMS Logistics to an or customer organisation's business and therefore needs to be protected appropriately. Information assets includes hardware (including desktop, laptop, tablet computers and mobile devices), software (both purchased and licensed but also freeware), information (not limited to electronic media such as databases, websites, electronic files but also paper and other forms including unrepresented information in the form of knowledge of the employees).

Responsibilities: RETEMS Logistics will:

- Familiarize the staff with their responsibilities in regards to reporting any concerns related to any issue which has to be improved;
- Regularly review employees' reports, concerns, complaints and suggestions;
- Conduct investigation of raised issues and take appropriate corrective actions;
- Ensure the anonymity, of all persons who choose to report and remain unknown;
- Protect reporter(s) from any pressure, harassment or victimization.

Expectations from interested parties: We expect and request our Competitors, Customers, Suppliers and other external interested parties to comply with expectations and relevant requirements related to Information Security.

Reporting: Our employees shall immediately report to management about any Information Security issues. Any person reporting a suspected violation of this policy will never be subject to disciplinary action or retaliation for the act of making the report.

Confidentiality: If reporter does not feel comfortable stating his/her name – he/she can make report confidentially. No attempt from management will be made to identify the individual. Information provided by the individual, or obtained in the course of investigation, will be treated as confidential to the extent permitted by law.

Disciplinary measures: Any our employee or partner which violates these requirements in connection with RETEMS Logistics business will be subject to disciplinary measures, up to and including termination of labor contract in the case of an employee, or termination of business relations in the case of an external party and, where appropriate, referral of the matter to relevant law enforcement authorities.

Communication: The Information Security policy principles will regularly be communicated and available to staff at all times. To involve our Customers, and any interested parties with a legitimate interest in our commitment, this Policy Statement is made available on our website **https://retemsgroup.com/**

Director: Sema Mehdiyev **Date: 21.11.2022**