Scope of services: RETEMS Logistics is a provider of International Freight Forwarding, Warehousing and Customs Clearance Services.
This policy applies to all individuals who engage with the third-party suppliers on behalf of RETEMS Logistics. Where these standards are not followed, this should be highlighted to the Director, Line Manager.

Statement: The purpose of this policy is to describe the IT security requirements and assessments to be completed for all information assets prior to implementation within RETEMS Logistics environment. Some information assets may require reassessment at various points of the asset lifecycle depending on their assigned classification.

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).
- **Third-Party** - Any individual, entity or corporation that is not a user. Any RETEMS Logistics contracted service, supplier, vendor and third-party sub-contractor who provides IT services which include the storage, transfer, security, management, procurement, operation or decommissioning of RETEMS Logistics information assets and associated data.

Responsibilities: Director shall:

- Ensure that third-party Suppliers requirements are determined;
- Ensure that third-party Suppliers requirements are passed the assessments.

Expectations from interested parties: We expect and request our third-party Suppliers to comply with expectations and relevant requirements related to IT security requirements.

Reporting: Our employees shall immediately report to management about any IT 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 third-party Suppliers which violate IT security 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 third-party and, where appropriate, referral of the matter to relevant law enforcement authorities.

Communication: The IT Risk Management policy for Third Party information will regularly be communicated and available to staff and third-party 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

*This document is owned by «**RETEMS LOGISTICS**» LLC, and its content may not be disclosed to third parties or reproduced without the written permission of the quality management representative*