Information Security Policy:

- Global Safety Textiles (“GST”) is aware of the importance and significance of the information security for our stakeholders and all our interested parties.

- We are committed to develop, deploy, and comply with this Information Security Policy with the objective of protecting the confidentiality, integrity, and availability of the information assets.

- This Information Security Policy applies to the entire GST organization, its personnel, contractors, visitors and third parties.

- The responsibilities of the Information Security Policy and processes are defined, shared, published, and accepted by each one of the employees, contractors and/or third parties.

- GST`s Global Management Board is responsible for approving this Information Security Policy to ensure that the Information Security requirements are met.

The information security requirements have been determined and documented. These requirements are based on the following objectives:

1. **Organization of information security:** We define, implement, and continuously improve an Information Security Management System (“ISMS”), supported by information security policies, procedures, and instructions aligned to the business goals, needs, contractual, and regulatory requirements. Including a clear definition of responsibilities, regulation of external IT services, availability of resources, and requirements for project management process. The effectiveness of the ISMS is regularly reviewed by top management through the monitoring of key process indicators.

2. **Asset management:** We identify and classify information assets and supportive assets to provide the adequate protective measures according to its protection objectives and needs. We define the responsibilities for their protection. Protective measures include evaluation and approval of external IT services. Only evaluated and approved software is used for processing the organization’s information assets.

3. **Risk management:** We implement a timely detection, assessment and addressing of risks to achieve the protection objectives for information security. We establish adequate measures for protecting the information assets under consideration of the associated opportunities and risks.

4. **Assessments:** We review Information security requirements, policies, and procedures at periodic intervals. An external provider conducts independent information security assessments at regular intervals and when fundamentals changes occur.

5. **Incident and crisis management:** We process and manage information security events (or observations) to limit their potential damage and prevent recurrence. We have contingency plans in place which consider information security risks in crisis situations. Including communication to relevant internal and external parties, when applicable.

6. **Human Resources:** We ensure that employees are suitable and competent for their positions and roles. All employees are committed and contractually bound to comply with information security policies, they are regularly trained and made aware of the information security requirements and the consequences of misconduct and violations. We determine and fulfill the requirements for teleworking.

Information Security Policy:

7. **Physical security:** We implement protective measures for identified security zones to protect information assets. We determine and fulfill the requirements for handling supporting assets during their entire lifecycle, including mobile IT devices and mobile data storage devices.

8. **Identity management:** Only securely identified (authenticated) users have access to IT services and IT systems. We define and implement a policy for handling login information. Users are accountable for safeguarding their authentication information.

9. **Access management:** We implement physical and electronic access control, as required. We determine and fulfill the requirements for managing of access rights.

10. **Cryptography:** We ensure proper and effective use of cryptographic procedures to protect information according to its protection objectives and needs. We use suitable measures during information transportation in public or private networks.

11. **Operations security:** We define operational procedures and responsibilities to ensure correct and secure operations, including change management, development and testing environments separated from operational environments, protection from malware and other cyber-attacks, events logs, management of vulnerabilities, information systems audits, and management of networks. Continuity planning for IT services is part of an overall program for achieving continuity of operations. Backup and recovery of data and IT services is guaranteed.

12. **System acquisition and development:** We consider information security requirements during the development or acquisition of IT systems. We determine and fulfill the requirements of network services. We protect the security of the information systems across their entire lifecycle, including in shared external IT services.

13. **Supplier relationships:** We maintain, by contractual and non-disclosure agreements, an appropriate level of information security while collaborating with suppliers and/or contractors.

14. **Compliance:** We define, implement, and communicate policies regarding compliance with the legal, regulatory, and contractual requirements and specifications related to information security. Including privacy and protection of personal data, where applicable.

This information security policy is communicated and available to employees and external relevant partners. They are also informed of any relevant changes.

Failure to comply with this Information Security Policy may result in consequences under the respective (labor) law.

GLOBAL SAFETY TEXTILES