**Trasta ESG Consulting Inc.**

**Information Security and Cyber Security Policy**

1. Purpose and Scope

Trasta ESG's mission is to create a clear and comprehensive framework to protect its assets, customer data, and information systems against cyber threats. The policy comes into force with the aim of defining information security and cyber security requirements, importance and application. It summarizes its determination to create and maintain a secure and resilient infrastructure against cyber threats, to ensure the security of corporate and customer information, and to protect customer trust.

This policy covers information systems processes and infrastructure, all employees, third-party suppliers, consultants, and all stakeholders who have access to corporate systems, data or technology resources. The parties from which the external service is received are responsible for the evaluation and management of the security risks that the services to be received from external services and suppliers will cause for the company.

2. Principles of Practice

Confidentiality: Only authorized persons can access all information in the company's business processes, and it is forbidden to share it with unauthorized persons.

Integrity: All data and systems cannot be altered accidentally or intentionally; Data integrity is maintained, data loss and corruption are prevented.

Authentication and Authorization: Users only have the access rights defined for them and act in accordance with the authentication processes.

Training and Awareness: Information security and cyber security awareness trainings are given to all employees on a regular basis; Information is provided about security vulnerabilities and threats.

3. Security Policies

Access Control: Users can only access information and systems that are necessary to perform their job functions.

Data Encryption: Sensitive data should be encrypted during transmission and when stored.

Password Management: Strong password policies should be implemented and updated regularly.

Firewall and Antivirus Software: All systems should be protected with up-to-date firewall and antivirus software.

Physical Security: Physical access controls must be implemented, and all computing devices must be properly protected.

## 3. Responsibilities

Management is responsible for providing the necessary resources in the field of information security and cyber security and supervising the effective implementation of security policies. In this context, it establishes the company's security standards and continuously monitors whether compliance with these standards is ensured. Unit managers, on the other hand, are responsible for the correct implementation of security policies in their departments, the correct assessment of security risks and the regular information of their employees. All employees must comply with the information security and cybersecurity policies set by the company; They also have an obligation to report immediately in the event of any security threat or breach. Disciplinary processes may be applied for employees who do not comply with these safety policies. It is the responsibility of the IT department to secure the technological infrastructure, keep the systems up-to-date, provide network security, take precautions against cyber attacks and minimize the impact of violations. Third parties cooperating with the company are obliged to comply with the specified security measures and must fulfill their security responsibilities within the framework of their contracts with the company.

## 4. Enforcement

This policy enters into force from the date it is approved by the company management and is binding on all employees. This policy will be reviewed annually and updated as necessary in light of the evolution of cyber threats and the changing of regulatory requirements. Any changes to the policy's enforcement process will be determined by the company's security needs.