INFORMATION SECURITY STATEMENT

PUBLIC

INFORMATION SECURITY STATEMENT

The objective of this statement is to provide executive direction for the protection of information owned by CES, investors, customers, employees, partners or suppliers, in whatever form it may be held or communicated, whether verbal, on paper or electronic. Information is one of our most valuable assets. Of equal value is the trust of our partners, employees and customers that we will protect the information that they have shared with us.

CES proprietary, investor, customer, partner, employee or supplier information, when created, stored, transmitted or communicated, must be protected from unauthorised access, use, modification or destruction. Consequently, all access to, and use of this information and data, requires adherence to the following policy principles:

Confidentiality: Appropriate measures must be taken to ensure that information is accessible only to those authorised to have access.

Integrity: The accuracy and completeness of information must be maintained and all changes or modifications affecting that information must be authorised, controlled, and validated.

Availability: Information must be available to authorised individuals when required. In the event of a disaster or other events, CES information and the systems critical to the success of our business must be recoverable in accordance with plans.

Authentication: All persons and systems seeking access to information or to our networked computer resources must first establish their identity by CES requirements.

Access Control: The privilege to view or modify information, computer programs, or the systems on which the information resides, must be restricted to only those whose job functions absolutely require it.

Auditing: User access to information, and activity on the Company's computers, smartphones, servers, production automation systems, firewalls, networks and physical security systems (such as CCTV etc.) must be recorded and maintained in compliance with all security, retention, relevant legislation and regulatory requirements.

Compliance: CES will comply with all relevant legislation and regulatory requirements regarding the management and security of information within its jurisdiction.

CES has established Information Technology Risk Management Plan, with supporting programs to achieve a certification to the Information Security Management Systems (ISMS) Standard – ISO 27001:2017; the practices of the corporation will meet this standard and will follow a programme of continuous improvement.

Security policies will be developed to support the ISMS objectives, together with detailed procedures. The ISMS will be complemented with the other Information Security policies and practices to achieve a holistic approach for Information Security.

The Chief Information Security Officer's department has the responsibility for development and maintenance of the Security Policies, which will be reviewed annually by the Corporate Risk Management Team and the Directors of CES.

All managers are responsible for implementing the Security Policies within their areas, and for adherence thereof by their staff.