MERISTEM

INFORMATION SECURITY POLICY STATEMENT

INFORMATION SECURITY POLICY STATEMENT

Information is an important business asset, adds significant value to the company and needs to be protected from threats that could potentially disrupt business continuity. Meristem Securities Ltd has drafted an information security policy based on the ISO/IEC 27001:2013 standard that demonstrates its intent to protect her information assets against security threats and to minimize the impact of security incidents.

The purpose of this information security policy is to protect the Meristem's information assets from all threats, whether internal or external, deliberate or accidental.

The Policy Scope covers User authentication and password policy, Clear desk and clear screen policy, IT Network use policy and User authentication and password policy which encompasses all forms of Information Security such as data stored on computers, transmitted across networks, printed or written on paper, sent by fax, stored on media or spoken in conversation or over the telephone.

All managers are directly responsible for implementing the Policy within their business areas, and for ensuring their staff adheres to it.

It is the responsibility of each employee to adhere to the policy. Disciplinary processes will be applicable in those instances where staff fail to abide by this security policy

Meristem Securities Ltd. is committed to:

- Protecting the confidentiality, integrity and availability of her information asset;
- Complying with applicable legal, regulatory and other requirements regarding Intellectual property rights, Data protection and privacy of personal information;

- Establishing, implementing, maintaining, and continually improving the information security management system;
- Ensuring appropriate resources needed for the information security management system are available;
- Ensuring that all persons within the scope of the ISMS receive adequate Information Security training;
- Conducting a systematic review of performance on a regular basis to ensure information security objectives are met;
- Ensuring that all breaches of information security, actual or suspected are reported to the ISMS Manager and thoroughly investigated by the Incident management team.

The information security manager is responsible for maintaining the policy and providing support and advice during its implementation. The review of the Information Security Policy and related documents shall be performed on an annual basis or when significant changes occur to ensure suitability, adequacy, and effectiveness of the ISMS.

Approved by

Deputy Managing Director

Date: 09/11/2022