Barloworld
Leading brands

INFORMATION SECURITY AND RISK MANDATE

Preamble

Barloworld continues to mature its information security approach in line with the evolving threat landscape. A risk-based approach underscores the response to the cyber threat landscape to ensure practicality, affordability and necessity of mitigations and controls. The approach includes people, process and technology mechanisms aligned to regulatory and legal requirements taking into consideration the different geographies and industry verticals in which Barloworld operates.

The objectives of the information security approach are to:

- Protect the organisation's information assets from intentional or accidental internal leakage, interception or disclosure to unauthorised parties;
- Protect the reputation of the information assets by ensuring their integrity;
- Protect the information- and technology dependent business processes that are vulnerable to attack;
- Protect the availability of sensitive information assets that have a substantial impact on day-to-day operations and service delivery to stakeholders;
- Ensure networked information assets communicate only with trusted and verified parties;
- Enable the secure, trustworthy and enforceable exchange of information assets.

Mindful that despite a robust information security approach, breaches may be realised, relevant insurance cover has been effected to offset potential losses that may arise from cyber risk. No significant cyber breaches were detected in the past financial year. Robust IT Continuity Plans, which are tested continuously to ensure these remain adequate and effective, are in place.

Information Security and Risk Mandate

1 Barloworld is committed to preserving the confidentiality, integrity and availability of all forms of information used by the organisation and maintained on behalf of all stakeholders, including employees, business partners, customers and regulatory bodies. As a result, specific procedures are developed to help administer and manage the storage and processing of electronic information related to the proper and lawful conduct of business. These procedures address all computer and information management activities that could constitute a threat or risk to the ongoing proper activities of this organisation in such a way that risk is minimised or otherwise accepted by the executive of Barloworld.

2 The leader of the information security function or his/her designated representative is the controlling officer in charge of developing, maintaining, disseminating and measuring compliance with this mandate through the procedures and standards that are generated in response to this commitment.

3 To ensure that the importance of this mandate is communicated uniformly throughout the organisation, all members of the Barloworld executive discusses and ratifies, at least annually, this mandate as it relates to regulatory compliance, legal privacy protection and information protection.

4 This mandate is applicable to all computer equipment, network or data communications equipment, computer programs, procedures and support software, data storage devices and media. Employees, business partners and contract personnel who use any computer-related technology must be aware of the provisions and their requirements related to this mandate and supporting policies.

Approved by: Group Risk and Sustainability Committee	Date Approved: 23 March 2021

5 In addition, this mandate authorises the development of standards for personnel activities, incident prevention and reporting and compliance or audit reviews directed by appropriate regulations and commonly accepted business practices.

6 Changes necessary to reflect current technology and new methods for ensuring secure business procedures will be supplemented to existing procedures as often as necessary.

7 It is the duty of all employees and contractors to report any actions or conditions that appears to violate the spirit of this mandate.

8 The Barloworld Group Risk and Sustainability Committee oversees the effectiveness of the Information Security and Risk mandate and its execution, with independent assurance provided by the internal and external audit functions.