POLICIES FOR INFORMATION SECURITY

(Control 5.1)

Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to, and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business requirements, legal, statutory, regulatory, and contractual requirements.

Procedure

The Company has produced an Information Security Policy in line with the requirements of Clause 5.2 of ISO/IEC27001 and with Control 5.1 of ISO/IEC27002. This Policy has been made available to all interested parties and has been authorised by the CEO/Managing Director, Waldo Willemse.

Additional policies have been created by the Company covering the following topics:

a) access control.
b) physical and environmental security.
c) asset management.
d) information transfer.
e) networking security.
f) information security incident management.
g) backup.
h) cryptography and key management.
i) information classification and handling.
j) management of technical vulnerabilities.
k) secure development.

These policies have been authorised by the appropriate manager and are reviewed on a regular basis to ensure continued suitability and effectiveness. They are made available to all relevant interested parties.

The review of these policies includes assessing opportunities for improvement of the Company's policies and managing information security in response to changes to:

a) the Company's business strategy.
b) the Company's technical environment.
c) regulations, statutes, legislation, and contracts.
d) information security risks.
e) the current and projected information security threat environment.
f) lessons learned from information security events and incidents.

The review of policies for information security takes the results of management reviews and audits into account.

If any of the policies for information security are distributed outside the Company, care must be taken not to disclose confidential information.