bis henderson recruitment

DATA PROTECTION & INFORMATION SECURITY POLICY

INTRODUCTION

Bis Henderson regards the lawful and sensitive treatment of personal information and customer data as very important to successful operations. The Data Protection Policy is part of Bis Hendersons Information Security. It is in place to make every employee aware of their individual responsibilities and how information-centric legislation affects them; thus ensuring Bis Henderson fulfils its legal and regulatory responsibilities and maintain the confidence of our customers. Compliance with the Information Security Policy is endorsed by the Chief Operating Officer and is mandatory to all employees. The policy places responsibility on both the company and its employees to ensure that Bis Henderson works within the principles embodied in current legislative and regulatory requirements.

INFORMATION SECURITY

1. Information security creates the management culture and environment for protecting Bis Henderson information and that of its customers and candidates, with the aim of ensuring business continuity and of minimising the impact of damage from security incidents. Bis Henderson management is committed to protecting the Company's information in any form from all threats whether internal, external, deliberate or accidental.
2. Information takes many forms and may be stored on computers, transmitted via networks, printed out or written down or spoken. From a security perspective appropriate protection should be applied to all forms of information used to convey data, knowledge or ideas.

SCOPE

3. This procedure applies throughout the Company. The procedure sets out an Information Security Policy and describes the primary responsibilities for its implementation. The Information Security Policy must be accepted by all staff upon commencement of employment covers:

- Data Protection
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Mobile Telephone Use

- IT Security and Equipment Disposal
- Information Security
- Email
- Internet Access
- Software Licensing Compliance

PROCEDURE

Policy

4. The corporate policy on Information Security applies to all Bis Henderson IT systems, information and locations (including home and customer premises) and is set out below.

- Bis Henderson will produce standards to support this Policy and include the relevant procedures and controls for implementation.
- Bis Henderson will assure confidentiality by protecting sensitive or valuable information from unauthorised disclosure or intelligible interruption by physical and other measures including appropriate classification and security markings.
- Bis Henderson will maintain the integrity of information by safeguarding its accuracy and completeness and protecting against unauthorised modification.
- Bis Henderson will meet business requirements for the availability of information and information systems.
- Bis Henderson will prevent and detect Viruses and other malicious software.
- Bis Henderson will meet regulatory, legislative and contractual requirements.
- Bis Henderson will plan to ensure the continuity and availability of essential services. The plans produced will be protected.
- Bis Henderson will make information security training available to all staff.
- Bis Henderson will ensure that all breaches of information security, actual or suspected, are reported and investigated.

Responsibilities

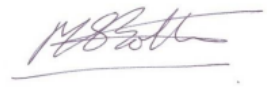
5. Bis Henderson's Chief Operating Officer is responsible for the definition of the outline Information Security Policy and reviews and agrees updates this with the Company's board on periodic basis. The Chief Operating Officer and a designated team member produces and maintains Information Security Procedures and provides advice and guidance to staff on their implementation, records and investigates all security breaches and recommends remedial action.

6. All Bis Henderson employees are responsible for implementing Information Security Policy and to be fully familiar of its requirements and application.

7. All Bis Henderson employees are contractually obliged to be aware of and comply with Information Security Policy and to report all security incidents.

Review and evaluation

8. The Chief Operating Officer will review this Policy and associated documentation as appropriate and is responsible for the maintenance of Policy documentation.



Mark Botham
Chief Operating Officer
July 2014