Statement of Guidance

Use of The Internet

1. Statement of Objectives

In its regulation of licensees' business conducted using the Internet, the Authority will wherever possible exercise a consistent approach as is used for business done through traditional media. Although existing laws and regulation can apply to business conducted through the Internet, including the Electronic Transactions Law 2000, there is a need for guidance to address the issues and risks specifically posed.

2. Business Plan Changes

2.1. In accordance with current requirements for business plan changes, licensees should inform the Authority before making additional or material changes to the services and products that differ from those in its original application.

2.2. The use of an Internet website for advertising purposes, in itself, does not constitute a change to the service or products offered. However, any interactive service such as the ability to purchase products or use money transmission facilities, for example, over the Internet would amount to at least a material change to the service, or additional changes to products, or product types.

3. Anti-money laundering Considerations

Licensees must have adequate policies and procedures in place to ensure compliance with the Money Laundering Regulations 2000. Licensees should review and amend if necessary these policies and procedures when making changes to the manner in which business is conducted, in particular the media utilised. Banking and investment business on the Internet adds a new dimension to Financial Services Providers' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for money laundering, and fraud.

4. Board and management oversight

4.1. Licensees should establish effective management oversight of the risk associated with Internet activities, including the establishment of policies to address accountability and controls to manage the risk.

4.2. It is crucial for the senior management of licensees to issue and maintain, on an ongoing basis, comprehensive information security policies relating to the use of technology in general and to transactional financial services in particular. The documents should set forth the policies, procedures and controls to safeguard the institutions' operations against security breaches, define individual responsibilities, and describe enforcement and disciplinary actions for non-compliance.

4.3. Licensees should review and approve the key aspects of its security control process.

4.4. The Board of Directors and senior management should oversee the development and continued maintenance of a security control infrastructure that properly safeguards Internet systems and data from both internal and external threats. This should include establishing appropriate authorisation privileges, logical and physical access controls, an adequate security infrastructure to maintain appropriate boundaries and restrictions on both internal and external user activities.

4.5. Licensees should establish a comprehensive and ongoing due diligence and oversight process for managing the institutions outsourcing relationships and other third-party dependencies supporting Internet activities.

4.6. A comprehensive process for managing the risks associated with outsourcing and third party dependencies is necessary. This process should encompass the third-party activities that may have a material impact on the licensee.

5. Security controls

5.1. Authentication and Authorisation

5.1.1 Licensees should adopt appropriate measures to authenticate the identity and authority of customers with whom it conducts business over the Internet.

5.1.2 Licensees should use reliable methods for verifying the identity and authority of new and existing customers seeking to initiate electronic transactions.

5.2. Segregation of Duties

5.2.1 Licensees should ensure that appropriate measures are in place to promote adequate segregation of duties within their Internet systems, databases and applications. These should be designed to reduce the risk of fraud in operational processes and systems and ensure that transactions and company assets are properly authorised, recorded and safeguarded.

5.2.2 In order to maintain segregation of duties, licensees need also to strictly control authorisation and access privileges.

5.3. Data Integrity

Licensees should ensure that appropriate measures are in place to protect the data integrity of Internet transactions, records and information.

5.4. Audit Trails

Licensees should ensure that clear audit trails exist for all Internet transactions. In particular, effective internal controls are needed in highly automated environments, but also that the controls can be independently audited, particularly for all critical Internet events and applications.

5.5. Confidentiality

Licensees should take appropriate measures to preserve the confidentiality of key information gathered over the Internet. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.

6. Legal and Reputational risk management

6.1. Adequate Information

Licensees should ensure that adequate information is provided on their websites to allow potential customers to make an informed assessment about the institution's identity, in particular the physical address of the licensee and its head office. As a matter of best practice licensees should state that it is regulated by the Authority and the home supervisor where applicable. There should be a prominent notification of this on the web pages displayed prior to entering into any Internet transaction.

6.2. Customer Privacy

Licensees should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the financial services provider is providing Internet products and services.

6.3. Incidence Response

Licensees should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks that may hamper the provision of Internet services.