BANK OF MAURITIUS

Guideline on
Internet Banking

February 2001

Guideline on Internet Banking

1. Preface

This guideline is issued to domestic banks and offshore banks under the authority of the Bank of Mauritius Act and the Banking Act 1988.

It is important that the banking industry in Mauritius adopts all desirable leading edge technologies in providing banking services to its customers. As a regulator of banks, the Bank of Mauritius has an important interest in ensuring that the banking services, including Internet banking, evolve in an orderly fashion with public interest in mind.

All licensed institutions are allowed to establish informational websites as defined in the guideline without seeking approval of the Bank of Mauritius. They must, however, advise the Bank in writing at least one month prior to the implementation of the website. The institutions proposing to launch communicative or transactional websites, are required to obtain prior written approval of the Bank of Mauritius.

An institution which has obtained approval to launch communicative or transactional websites will have its website posted on that of the Bank of Mauritius so as to allow the public to verify that the website belongs to an institution licensed under the Banking Act 1988.

This guideline will come into effect on 2 April 2001.

2. Interpretation

"Internet banking" refers to banking products and services offered by institutions on the Internet through access devices, including personal computers and other intelligent devices.

"Internet banking services" means products and services normally offered by institutions under their respective licences through the Internet.

"Institution" means a domestic bank or an offshore bank licensed under the Banking Act 1988 that has received or applied for approval to establish a communicative or transactional website.

"Communicative website" means a website which allows some interaction between the institution's systems and customers, both existing and potential. Customers may send information and make enquiries about their accounts. The communication may take the form of e-mail, on-line forms, making account enquiries or static file updates (e.g. name and address changes).

"Informational website" means a website which is intended to disseminate general information about the institution and to advertise its products and services, but which provides no interactive capability.

"Transactional website" means a website which allows customers to execute banking transactions, in addition to the services that are offered by a "communicative website" or "informational website".

3. Scope of the Guideline

The guideline sets out a regulatory framework for providing Internet banking services in Mauritius. It lays down the minimum standards that the institutions must observe regarding Internet banking and prescribes the requirements and the processes for obtaining the Bank of Mauritius approval for establishing Internet banking services. The institutions are free to adopt standards, systems and practices more stringent than those outlined in the guideline to suit their particular circumstances.

4. Objective

The objective of this guideline is to require the institutions to establish systems and practices for internet banking designed to:

- limiting systemic and other risks that could threaten the stability of financial markets or undermine confidence in the payment system;
- encouraging institutions to educate customers about their rights and responsibilities and how to protect their own privacy on the Internet; and
- encouraging the development of effective, low risk, low cost and convenient payment and financial services to customers and businesses through the Internet.

5. Approval of Bank of Mauritius

An institution seeking to launch its own communicative and/or transactional website or to utilise the communicative and/or transactional website of a third party, is required to obtain the prior written approval of the Bank of Mauritius. In this regard, the documents and information listed below shall be submitted to the Bank of Mauritius at least one month prior to the proposed launching of communicative and/or transactional websites along with the request for the Bank's approval:

(i) Confirmation by the Chairperson of the board of directors of the institution, (Chief Executive Officer in the case of a foreign bank branch) that it is ready to provide Internet banking (as per annexure);

(ii) Business and strategic plans on Internet banking (for at least two years);

(iii) Internet security arrangements and policy;

(iv) Risk Management framework;

(v) Terms and conditions for Internet Banking Services;

(vi) Client Charter on Internet banking;

(vii) Privacy Policy Statement; and

(viii) Any outsourcing or website link arrangements, or strategic alliances or partnerships with third parties that have been finalised.

An institution which has obtained approval to operate a communicative or transactional website should submit the following information to the Bank of Mauritius **within two weeks** after obtaining Bank of Mauritius approval or a week prior to the launching of the website, whichever is the later:

- Letter providing its website address, confirming the validity of its site and authorising the inclusion of its site in the web page of the Bank of Mauritius; and
- a soft copy of the institution's logo to be included in Bank of Mauritius' site.

6. Reporting

An institution operating a communicative or transactional website shall report to the Bank of Mauritius on its performance in achieving the objectives set out in its strategic and business plans, including a brief overview of its risk management processes respecting Internet banking. It shall submit to the Bank copies of its security program and contingency and business resumption plans at the end of each financial year beginning with the financial year ending 30 June 2001.

7. Internet banking risks

Internet banking risks can adversely impact on an institution's earnings and capital. Therefore, an institution offering Internet banking services is required to implement proper and effective policies, procedures and controls to protect information and ensure its integrity, availability and confidentiality. To assist institutions to properly identify, quantify and manage risks associated with Internet banking, it is recommended that such risks be categorised as follows.

(i) ***Strategic risk***

Strategic risk stems from inappropriate business decision and/or incorrect implementation of decisions.

An institution may incur substantial loss/wastage of its resources as a result of incorrect choices or decisions regarding its Internet banking strategy.

The institution should conduct a feasibility study prior to initiating on Internet financial services.

(ii) ***Transaction risk***

Transaction risk results from flaws in system design, implementation or ineffective monitoring leading to frauds, errors and failures to provide banking products and services. To control transaction risk there is need for adequate security and monitoring of the Internet banking system.

An institution must have in place preventive and detective controls to ward off its Internet banking systems from any unauthorised use, both internally and externally.

Adequate operating policies and procedures, auditing standards, effective risk monitoring processes including contingency and business resumption plans should be implemented.

(iii) ***Compliance risk***

Compliance risk arises from failure to observe laws, rules, regulations, prescribed practices or ethical standards when delivering Internet banking services.

The Internet banking service should be designed and operated in such a manner that it always complies with all relevant laws and guidelines.

Every institution should state clearly in its Terms and Conditions for Internet Banking Services and on its website that the governing law is the Mauritian law.

(iv) ***Reputation risk***

Reputation risk occurs when systems or products do not work as expected and cause widespread negative public reaction. Internet banking systems that are poorly executed would present this risk. An institution's reputation may also be affected if its Internet banking system is unreliable or inefficient or the products and services offered are not presented in a fair and accurate manner.

Adverse public opinion may create a lasting, negative public image on the institution's overall operations, which may impair the institution's ability to establish new relationships or services or continue servicing existing customers and business relationships.

An institution should undertake immediate and effective remedies to address operational failures or unauthorised intrusions and ensure that timely steps are taken to address adverse customer and media reaction.

An institution should also educate and inform its customers on what they can reasonably expect from a product or service and the special risks and benefits that they will incur or obtain when using the system.

(v) ***Traditional banking risk***

An institution offering Internet banking services is faced with the same types of traditional banking risk such as credit risk, interest rate risk, liquidity risk, price risk and foreign exchange risk. The Internet may, however, heighten some of these risks.

An institution providing Internet services should therefore develop appropriate and adequate systems to manage the various types of traditional banking risks and maintain those systems on a regular basis.

8. Risk Management Framework

(i) ***Formulation of a policy***

The development of Internet banking widens the scope for increased interaction between institutions and their customers and opens up new avenues for cross-border banking transactions exposing institutions to additional risks. Many aspects of risks associated with Internet banking are neither fully discernible nor readily measurable.

Accordingly, each institution should develop a risk management framework that is comprehensive enough to deal with known risks and flexible enough to accommodate changes. It should be subject to appropriate oversight by the board of directors and senior management. The sophistication of the risk management processes should be appropriate for the institution's level of risk exposure.

(ii) ***Role of Board of Directors***

The board of directors shall

- approve the Internet banking strategy of the institution to ensure that it is consistent with the institution's strategic and business plan;
- approve contingency and business resumption plans that should be in place before an institution launches the Internet banking services .
- set the level of Internet banking risk and review, approve and monitor Internet banking technology related projects that may have significant impact on the institution;
- ensure that the Internet banking systems are operated in a safe and sound manner, including the availability of contingency and business resumption plans;
- review and approve the information security policies;
- ensure that an adequate system of internal controls is established and maintained;
- ensure that qualified and competent persons at senior level are employed to identify, monitor and control Internet banking risks and that the effectiveness of the internal control system is monitored on a regular basis; and
- carry out an active oversight of the management of Internet banking risk of the institution by regularly receiving comprehensive written reports identifying material risks.

In carrying out the above responsibilities, the board may engage the services of outside experts, as needed.

(iii) ***Role of Management***

The senior management should ensure that

- the Internet banking products are consistent with the institution's overall strategic plans and the risks and ramifications of offering such products over the Internet are within the institution's risk tolerance;

- necessary steps are taken to identify, monitor and control Internet banking risk and monitor the effectiveness of the internal control system;

- the Internet banking system is designed and operated in a manner that complies with all relevant laws. Senior management should also monitor developments and changes in consumer and banking laws, regulations and interpretative rulings and take adequate measures to comply with them;

- the overall effectiveness of the institution's internal controls is continually monitored. There should be a proper system to track and report internal control weaknesses for prompt corrective measures;

- adequate operating policies and procedures, auditing standards, effective risk monitoring processes, contingency and business resumption plans are available;

- adequate and comprehensive reports are provided to the directors for decision making;

- adequate expertise and resources are available to operate and maintain their Internet banking system; and

- effective channels of communication are established so that the employees are fully aware of policies and procedures affecting their duties and responsibilities, including a clear delineation of lines of authority and responsibilities for managing Internet banking risks.

9. Security policy

Each institution shall establish a written policy on the overall security of its Internet banking system.

Security Requirements

Each institution must have a security program providing for the security arrangements which should achieve the following objectives.

- Data privacy and confidentiality.
- Data integrity.
- Authentication/identification of counterparties.
- Non-repudiation of Internet banking transactions.
- Access control/system design to prevent unauthorised access attempts.
- Business continuity plan.

An institution must have the following minimum security controls. However, it is the institution's responsibility to ensure that its security controls are complete in the light of its specific circumstances. As such, it could have additional security controls.

(i) ***Network and Data Access Controls***

Each institution should apply adequate access controls to protect its network, applications and data from unauthorised parties.

Access controls should be designed to effectively restrict unauthorised individuals from entering sensitive data, retrieving confidential information or enabling access to bank software applications and operating systems.

(ii) ***User Authentication***

Each institution should put in place tested systems to securely authenticate the identity of Internet banking customers when customers access personal account information or engage in on-line transactions for products or services.

Each institution should provide sufficient authentication for Internet banking customers who access personal account information or engage in online transactions for products or services.

The authentication processes should be reviewed and periodically tested for effectiveness through penetration testing and other monitoring methods.

Senior management should keep abreast of new or developing standards which may affect the institution's existing use of authentication devices and processes.

Each institution should use a combination of access, authentication and other security controls to create a secure and confidential Internet banking environment. These generally include passwords, firewalls, and encryption.

(iii) ***Transaction Verification***

Each institution should implement Internet banking agreements which clearly define the procedures for valid and authentic electronic communications between its customers and itself. The agreements should specify that the parties intend to be bound by communications that comply with these procedures.

Each institution should maintain audit trails of all transactions to enable the verification of specific transaction and provide evidence in the event a transaction is repudiated by its customers.

(iv) ***Virus protection***

Senior management should implement a detection and prevention program to minimise the possibility of computer viruses. This program should at least include end-user policies, training and awareness programs, virus detection tools and enforcement procedures.

(v) ***Detection of possible intrusions***

Each institution should make effective use of monitoring tools to identify vulnerabilities of its Internet banking system and in a real-time mode, detect possible intrusions from external and internal parties. In this regard, each institution is required to conduct penetration testing and administer manual or automated intrusion detection processes.

a) ***Penetration testing***

Each institution should use penetration testing to identify, isolate, and confirm possible flaws in the design and implementation of passwords, firewalls, encryption, and other security controls. The testing should be conducted by an objective, qualified, internal or external source prior to the introduction of Internet banking and at least once a year or whenever substantial changes are made to the Internet banking security systems.

b) ***Intrusion Detection***

Each institution should set up strong intrusion detection devices to control network traffic on a real-time basis. The intrusion detection system must withstand outside attacks and be capable of identifying and reporting departures from normal processing. Adequate audit trail mechanisms should be in place to prevent internal fraud, and provide the means to detect unauthorised intrusion or transactions.

Each institution should ensure that it has a combination of regular monitoring of network activity, a well-configured firewall, and regular reminders of its security policies. The institution's security policy should make it incumbent on its responsible officers to report security breaches **promptly** to a nominated member of senior management and to the Bank of Mauritius.

10. Internet banking security program

Each institution shall establish a written policy on the overall security of its Internet banking system.

Each institution shall further implement an overall security program which should incorporate the institution's risk management controls. The security program should set out the policies, procedures and controls to safeguard the institution's information, define individual responsibilities, and describe enforcement and disciplinary actions for non-compliance.

The security program should establish the necessary organisation structure and accountability in the process of the management of risks associated with Internet banking. The need to create awareness throughout the organisation that security is an important cultural value should also be ingrained in the security program. Every institution should ensure that adequate training is provided to the relevant staff to keep them updated on new security risks and methods of mitigating such risks.

Senior management should carry out regular security risk assessments to track down internal and external threats that may undermine data integrity, interfere with service or result in the destruction of information.

Every institution should establish specific reporting requirements for security breaches.

Senior management should ensure that the security measures instituted are current and properly implemented and comprehensive security policies and procedures are stringently enforced.

An institution should adopt a security awareness program to give users a clear understanding of the procedures and controls necessary for a secure environment. This security awareness program should strengthen the institution's security policy and program and may include, for example, instructions regarding password protection, Internet security procedures, user responsibilities and employee disciplinary actions.

11. Contingent and Business Resumption Plans

The contingent and business resumption plans should be approved by the board of directors prior to the launching of Internet banking services . They should include measures covering data recovery, alternate data processing capabilities, emergency staffing and a public relations and outreach strategy to respond promptly to customer and media reaction to system failure and unauthorised intrusions.

Each institution should evaluate and determine the importance of the business applications and processes and establish in order of importance business resumption designed to recover the most critical functions and systems.

Each institution should also establish procedures to be followed in the event its competitors which rely on similar technology, experience operational failure.

The back-up systems should be fully maintained and tested on a regular basis to minimise the risk of system failures and unauthorised intrusions. It is expected that security and internal controls at the back-up locations should be as sophisticated as those at the primary processing site.

Any intrusion, attempted intrusion or suspicious activity should be immediately reported to the nominated member of senior management for prompt corrective measure, followed by a report to the Bank of Mauritius.

12. Outsourcing

Each institution may outsource its Internet banking systems to resident and non-resident (i.e. located outside Mauritius) service providers and software vendors subject to the prior written approval of the Bank of Mauritius and the following conditions:

(i) The decision taking function of an institution should remain with it and the process to be outsourced should not threaten its strategic flexibility and its process control;

(ii) The image, integrity and credibility of the institution should not be impaired by the outsourcing arrangement;

(iii) The institution should be able to manage risks associated with these new relationships;

(iv) Appropriate oversight program should be set up to monitor the outsourcing vendor's controls, condition and performance; and

(v) There should be adequate undertaking for regular servicing by the supplier.

Each institution should continue to remain responsible for the performance and actions of its outsourcing vendors in relation to the services outsourced by the institution.

Each institution should be aware of the privacy concerns and its obligations for any loss of control of customers' information.

Before contracting any Internet banking service, each institution should fulfil the following conditions:

(i) The institution should perform sufficient due diligence to satisfy itself of the outsourcing vendor's expertise, experience and financial strength to fulfil the obligations;

(ii) The written approval of the Board of Directors should be obtained to outsource the Internet banking system to the service provider or software vendor;

(iii) The ownership and control of bank records should remain with the institution;

(iv) The institution should enter into a service agreement with the outsourcing vendor with a clause on professional ethics and conduct in performing his duties. It should be clearly stipulated in the service agreement that it reserves the right to terminate the services of the outsourcing vendor if it fails to comply with the conditions imposed. The service agreement should also clearly delineate the roles, responsibilities and accountability of each party;

(v) The institution should carry out a risk assessment of such arrangements which should ensure that adequate back-up arrangements such as alternative service providers are available;

(vi) The institution should have the ability to exercise the necessary control to properly manage the outsourced system for providing the Internet banking services;

(vii) The institution should put in place proper reporting and monitoring mechanisms to ensure that the integrity and quality of work conducted by the outsourcing vendor is maintained. Regular testing and review of the work done by the outsourcing vendor must be conducted;

(viii) The external and internal auditors of the institution should have the ability to review the books of the outsourcing vendor and perform audits or obtain from the outsourcing vendor independent internal control audit reports. Any weaknesses highlighted during the audit must be well-documented and promptly rectified especially where such weaknesses may affect the integrity of the internal controls of the institution; and

(ix) The details of the outsourcing arrangement should be forwarded for approval by the Bank of Mauritius **at least two weeks** before entering into

an agreement with the service provider, indicating whether all of the abovementioned requirements are satisfied.

13. Advertisements and website links

An institution will not require the prior approval of the Bank of Mauritius for advertisements or web linking arrangements made on its website, provided that such advertisements do not fall within the ambit of section 38 of the Banking Act 1988. The institution should, however, keep the Bank of Mauritius informed of such advertisement arrangements.

(i) ***Advertisements by an institution on third party websites***

This guideline does not seek to restrict the advertisement and posting of financial product information of an institution on third party websites including those of institutions operating outside Mauritius. However, each institution should ensure that it has the necessary controls in place to manage risks associated with the third-party websites.

The advertisement should be monitored for completeness, accuracy and timeliness.

An institution is advised to notify its customers regarding the websites that it will use to advertise its products and services and to caution them that information contained in any unauthorised third party websites may be incomplete, inaccurate or outdated.

An institution is encouraged to adopt additional procedures to safeguard its customers' and its own interests.

(ii) ***Website links***

When an institution provides links to third party websites to enable customers to access other third party services or products, the institution should analyse the risks presented by these arrangements.

In managing Compliance Risk, an institution providing hypertext links to third parties on its website should include a clear message to inform the customers that as soon as they leave its website the privacy policy of the institution would lapse.

The institution should advise customers to read its privacy policy statements and also use disclaimers to indicate that:

- A link to other websites is not an endorsement of those websites; and
- the institution makes no warranties as to the accuracy information available on those sites.

Where the link draws information from a third party's website into the institution's website, it is important that the institution clearly states the source of such information in order not to mislead or deceive users.

As part of its overall management policy, an institution should adequately manage its linking practices and enter into linking agreements where appropriate. The linking agreement should include the use and control of user data generated by the links as well as privacy and data protection obligations.

An institution providing hypertext links to third parties on its website or advertisement facilities to third parties should also have clear disclaimer statements informing customers that it is not responsible for the products and services offered by third parties.

14. Strategic alliances or partnership

An institution may enter into strategic alliances with partners in relation to the provision of Internet banking services.

An institution should ensure beforehand that the proposed alliances or partnerships do not result in any conflict of interest.

The details of alliance arrangements should be forwarded for approval to Bank of Mauritius **at least two weeks** before entering into an agreement with partners.

15. Customer Protection and Privacy Issues

(i) ***Customer Education***

Each institution should have a web page to educate customers on Internet banking particularly, with respect to their rights and responsibilities and the protection of their own privacy on the Internet.

Prior to the offering of Internet banking services to their customers, each institution is required to ensure that it has complied with the following:

a) The customers have agreed to the terms and conditions for Internet banking services;

b) The customers have been informed of the risks involved in the use of the Internet banking services ;

c) The customers know their rights and responsibilities and are fully aware that they are responsible for their own actions;

d) The customers have been informed that they may specify maximum limits for funds transfer to limit their risks;

e) The customers have been advised to read the privacy policy statements of the institution and third parties (refer to 13(ii) "Website links") prior to providing any personal information to the institution or third parties; and

f) The customers have been educated on their role to maintain security of their personal information by not sharing their IDs and passwords with anyone, by changing their passwords regularly, and by remembering to sign off.

(ii) ***Product Transparency***

Each institution should ensure that the products and services offered on the Internet are fairly and accurately disclosed. The features of the products and services, terms and

conditions including any fees, charges, penalties and relevant interest rates should be made transparent to the customers in plain language as far as possible. Any agreements or contracts should be made available in a form, which can be downloaded, printed and retained by a customer.

Each institution should provide advance notice to customers of variation of terms and conditions of the Internet banking services in relation to imposing or increasing charges, increasing the customer's liability for losses or any other material changes.

The terms and conditions for Internet banking services shall include the duties of the institution and customers, contractual arrangements for liability arising from unauthorised or fraudulent transactions, mode of notification of changes in terms and conditions and information relating to the lodgement of complaints, investigation and resolution procedures.

The contractual arrangements for liability should provide for sharing of risks between the institution and the customers. Customers should not be liable for loss not attributable to or not contributed by them.

Each institution should only enrol customers into a new product or service which involves a cost to the customers if it has been requested by the customers with full knowledge of the cost involved.

If an institution is found to have engaged in a conduct that is misleading or deceptive, or made a false or misleading representation with regard to its products and services, the Bank of Mauritius will not hesitate to take appropriate action against the institution.

(iii) ***Client Charter on Internet banking***

Each institution offering banking products and services over the Internet should have a Client Charter on Internet Banking.

The Client Charter should at the minimum state the institution's commitment towards ensuring safe operations, privacy of customer information, reliable and quality services, transparency of products and services, and prompt response for enquiries and complaints.

The Client Charter must be prominently displayed in the institution's website.

(iv) ***Privacy Policy***

Each institution should adopt a privacy policy which explicitly lays down its commitment to safeguard the privacy of customer personal information.

The privacy policy statement must

a) identify the types of information the institution collects about customers and how the information is used;

b) provide a brief description on the kind of existing security procedures that are in place or clearly state that sufficient safeguards have been put in place to protect the loss, misuse or alteration of information under the institution's control including restricting employee access to information, including that respecting a customer who has terminated his relationship with the institution;

c) identify with whom the institution shares this information, including agents, affiliates and non-affiliated third parties and how the institution ensures that the confidentiality of information is maintained;

d) explain the choices available to customers regarding collection, use and distribution of the information including the customers' right to opt-out of disclosures that are not mandatory;

e) explain how the institution maintains the accuracy of information and how customers can correct inaccuracies in the information; and

f) explain how the institution handles customer questions or complaints about the handling of personal information.

The referencing points or icons for the privacy policy statement should be prominently visible at specific locations on the institution's website where they may not be missed out by customers.

Each institution should at the minimum prompt customers to refer to its privacy policy statements prior to or at the time that individually identifiable information is collected.

(v) ***Customer Support Services and Enforcement Issues***

Each institution should supplement its privacy principles with a series of questions and answers about the handling of customer information.

Each institution should provide an e-mail link on its websites for privacy-related questions or complaints.

Each institution should supply customers with written hard copies of its privacy policies, in addition to using its website as a medium for communicating its privacy policies to customers.

Each institution should take steps to enhance its employees' understanding of compliance with such policies. The institution should ensure that its staff are aware of their responsibilities under the institution's privacy policies and information practices.

Each institution may also include its privacy policies into its code of ethics, and require the employees to certify their own compliance (annually or periodically) with the ethics code.

Each institution should set up procedures to address internal breaches to deter employee violations of the privacy policies.

Each institution should ensure that online privacy policies and information practices are consistent with its offline, or physical environment, information-collection activities.

Each institution should review its internal controls to ensure that these controls prevent the improper disclosure of personal information to third parties. Internal controls should incorporate a monitoring and review mechanism to test compliance with established privacy policies and information practices.

Each institution should disclose a procedure to enable customers to inquire about its personal information or inform the institution about the potential misuse of personal information in the online environment.

16. Compliance with other requirements

(i) ***"Know your customer policy"***

Each institution is required to have face to face interaction with customers prior to the opening of accounts or extension of credit.

Each institution should also develop its own specific know your customer rules as well as rules for scrutiny over transactions which should at least be as exhaustive as those implemented in a physical environment.

Each institution should also establish appropriate measures to adequately identify customers who are reached over third party websites.

The institution should take reasonable measures to ensure that the Internet banking facilities offered by it are not capable of being used to commit or facilitate an act of money laundering.

(ii) ***Maintenance of books and records***

The books and records should, at all times, be maintained in Mauritius for Bank of Mauritius' inspection.

17. Transitional period

Every institution already delivering Internet banking services will have to submit the information and documents mentioned in section 5 'Approval of the Bank of Mauritius' within six weeks after the coming into effect of this Guideline.

Bank of Mauritius
February 2001

Annexure

Attestation by the Chairperson on behalf of the Board of Directors of a locally incorporated bank/Chief Executive Officer of a foreign bank branch that the Institution is ready to provide Internet banking services.

Name of institution:……

I confirm that:

- ☐ Internet banking is consistent with the institution's strategic and business plans;
- ☐ The board of directors and senior management understand and are ready to assume the role and responsibilities stated in the guideline;
- ☐ Risk management process is subject to appropriate oversight by board of directors and senior management;
- ☐ The institution has put in place appropriate security measures and Internet banking security policy;
- ☐ The institution has established appropriate internal controls and performance measures for the monitoring of Internet banking products, services, delivery channel and processes;
- ☐ The Board of directors has approved the contingency and business resumption plans; and
- ☐ The institution has adequate resources to support the offering of Internet banking services.

Signed by:…….. Dated:……

Name of Chairperson/Chief Executive Officer