PART I - OVERVIEW

1. INTRODUCTION

1.1 The Internet's unique broad access in terms of geography, users, applications, databases and the connectivity of computer systems creates a whole host of new risks besides the existing traditional risks faced by an insurer in managing its internal computer systems. It is imperative, as such, that the insurer offering Internet insurance identifies and manages these Internet-related risks adequately. In view of the potential risks in Internet insurance, the Guidelines serve to prescribe the minimum requirements which insurers should observe in the provision of Internet insurance.

1.2 Whilst it is recognised that the Internet enhances the environment in which insurance products can be better advertised, bought, delivered and serviced, it **does not alter** the fundamental principle of protection of policy owners' interests. An insurer should not compromise on the conduct of its insurance activities on the Internet to the detriment of its financial position so as to be able to continue to meet its fiduciary obligations to the policy owners. An insurer is advised to be diligent at all times and adopt more stringent security measures beyond the minimum requirements recommended in the Guidelines. An insurer must also keep closely abreast with relevant developments in Internet insurance, including the developments in technological, legal, regulatory and customer-protection areas.

2. COVERAGE

2.1 The Guidelines apply to all licensed insurers that carry out Internet insurance activities. In addition to the Guidelines, licensees are also required to comply with GPIS 1: 'Guidelines on Management of IT Environment' and any other related circulars or guidelines that may be issued by the Bank from time to time. For the

purpose of the Guidelines, Internet insurance activities are defined to mean the use of the Internet as a channel to transact insurance business with customers or as a platform for transmission of customers' information. An insurer is required to seek the Bank's prior approval to conduct Internet insurance (details to be submitted are in **Appendix I**) together with an undertaking (attached in **Appendix II**) signed by the Chairman that the insurer is ready to provide Internet insurance.

2.2 The following types of Internet-based systems are not subject to the Guidelines:-

(a) use of e-mail via an Internet provider between the insurer and its customer on an ad-hoc basis for general enquiries only, for example, inquiry on status of policy and clarification on terms and conditions of the policy; and

(b) use of e-mail via an Internet provider within the company, for example between the insurer and its head office and branches, as well as between the insurer and its related parties, such as reinsurers, brokers and agents, which does not involve transmission of files containing customers' information.

3. TYPES OF INTERNET INSURANCE WEBSITES

3.1 Internet insurance sites can basically be categorised into two types, as follows:-

(a) **Information-based website**

It provides predefined publicly available marketing information of the insurer including the product and services offered. It may also enable policy owners make monologue e-mail contact with the insurer; and

(b) **Interactive-based website**

It provides for transactions to be executed including soliciting insurance proposal and the purchase and renewal of policies that may or may not involve online payments.

PART II - INTERNET INSURANCE RISKS

As a guide for the insurers to identify, quantify and manage Internet insurance risks, the types of Internet insurance risks can be categorised as follows:-

4. STRATEGIC RISK

4.1 Strategic risk arises when the overall implementation of Internet insurance is not in line with the vision and business objectives of the insurer. This risk can be a result of the Internet initiative not being driven and actively supported and lacking clear strategic direction from the top, and the lack of smooth coordination and understanding of the Internet's potential and implications between senior management and the people with the technological skills.

5. OPERATIONS RISK

5.1 Operations risk may include inaccurate forecast of customer volume or traffic, inappropriate management information systems and ineffectively managed outsourcing. Poor estimation of the volume of customer visits to the insurer's website, whether to view information or to transact, may impact on the performance and accessibility of the insurer's website. As such, scalability and the ease to increase capacity of the Internet insurance system are critical aspects for the insurer to manage under operations risk. Management information systems may not be upgraded appropriately to generate sufficient, meaningful and relevant information for timely management decision-making in insurance activities on the Internet. Outsourcing also poses risks due to, among others, potential loss of control of business activities by the insurer.

6. TRANSACTION RISK

6.1 This arises from deficiencies in system design, implementation or ineffective monitoring resulting in fraud, errors and the inability to deliver insurance products and services offered as agreed.

7. SECURITY RISK

7.1 Security risk can be categorised as follows:-

(a) **Data privacy and confidentiality risk**

Data may be monitored and read by unauthorised parties.

(b) **Data integrity risk**

Data may be altered or modified by unauthorised parties with malicious intent, thus compromising the insurer's databank and may affect the accuracy of product information, integrity of transactions and impact customers' confidence.

(c) **Authentication of users risk**

The anonymity of users in cyber space, including that of customers and the insurer renders risk in the authenticity of the parties to a transaction as to whether the parties are who they say they are.

(d) **Repudiation risk**

Customers may dispute the validity of, or refuse to acknowledge legitimate communications or transactions.

8. COMPLIANCE RISK

8.1 Compliance risk arises due to violation of laws, rules, regulations, prescribed practices or ethical standards which would result in among others, limited business opportunities, lack of customers' trust and lack of enforceability of contracts.

9. REPUTATION RISK

9.1 Reputation risk arises when systems, procedures or products do not work as expected and causes widespread negative public reaction. In an Internet-enabled business, such risk is heightened as the rapid dissemination of information means that any incident, good or bad, is common knowledge in a short space of time and

such news can be self-fulfilling prophecies. The insurer's reputation can be adversely affected if the insurance products and services offered on the net are unreliable, unfair and inaccurate resulting in misselling of such products and services. Being a service-oriented industry, adverse public opinion may impair the insurer's public image and its ability to establish new relationships with customers and/or maintain existing policy owners or even face litigation or material financial loss.

10. CONNECTIVITY RISK

10.1 The insurer must always bear in mind that the very efficiency rendered by the Internet with respect to ease and flow of information proffers a double-edged threat at the same time. The threat expands in line with the expansion of the network resulting in the systems becoming more vulnerable. The environment of interconnected computer systems can potentially create a systemic effect that offers a threat of total failure, incapacitation or compromise in the insurer's business activities.

11. TRADITIONAL INSURANCE RISK

11.1 Insurers whether offering offline or online insurance products and services face the same type of traditional insurance risks such as underwriting risk, reinsurance risk, claims risk, investment risk and legal risk. The offering of insurance products and services on the Internet may change the nature of these risks.

12. RESPONSIBILITY OF INTERNAL AUDIT

12.1 The internal audit departments of insurers are required to evaluate the risk impact and adequacy of the risk management framework for their Internet Insurance activities in respect of the risks listed above to ensure compliance with the minimum acceptable standards in the Guidelines.

PART III - RISK MANAGEMENT FRAMEWORK

13. RATIONALE

13.1 The Internet is a highly dynamic and accessible technology which continually poses considerations on security, legal, regulatory and customer protection issues. As such, an insurer should work towards a **written Risk Management Framework (RMF) that is comprehensive enough to address known risks and flexible and dynamic enough to quickly accommodate changes and address any new risks**. A sound RMF must have the full support and endorsement of the Board of Directors (BOD) and should incorporate the implementation of proper and effective policies, procedures and controls to effectively protect and ensure integrity, availability and confidentiality of information and transactions. The Guidelines should be adapted and enhanced to complement and address new risks in an environment of interconnected computer and systems created by the Internet technology. The RMF should cover the components listed in the following paragraphs.

14. ROLES AND RESPONSIBILITIES OF BOARD OF DIRECTORS

14.1 The **ultimate responsibility for the conduct of a sound Internet insurance business rests with the BOD**. The role and responsibilities of the BOD are to be undertaken and upheld in the spirit of good corporate governance and best practices as expounded in the BNM/RH/GL/003-2: Prudential Framework on Corporate Governance for Insurers (the Corporate Governance Framework). The BOD should apply the guiding principles in the Corporate Governance Framework at all times to promote sound management of the business and affairs of an insurer on the Internet.

14.2 Specifically, the roles and responsibilities of the BOD in Internet insurance should include:-

(a) to ensuring Internet insurance is conducted in a safe and sound manner;

(b) to provide effective strategic direction and approve the Internet insurance strategy or business model that may encompass product and service information for policy servicing and customer claims processing to ensure that it is in line with the insurer's strategic and business plans;

(c) to provide oversight, review and approve a sound internal system of security policies, procedures, limits and controls for managing material risks;

(d) to set the level of Internet insurance risk and review, approve and monitor Internet insurance-related projects that may have a significant impact on the insurer's risk appetite and risk profile;

(e) to oversee the conduct of Internet insurance business to ensure that it is properly managed to meet the insurer's corporate objectives and that the insurer's online dealings are equally fair and equitable as its offline insurance dealings;

(f) to approve corporate policies in critical areas of operations including underwriting, reinsurance and claims management for products and services offered on the Internet;

(g) to perform an active oversight of the management of Internet insurance risk by receiving regular information and briefings that identify the material risks; and

(h) to ensure that senior management takes the necessary steps to identify, monitor and control Internet insurance risks and monitor the effectiveness of the internal control system.

15. ROLES AND RESPONSIBILITIES OF SENIOR MANAGEMENT

15.1 Besides ensuring sound business practices consistent with good corporate governance principles as provided in the Corporate Governance Framework, the roles and responsibilities of the senior management in Internet insurance should specifically include:-

(a) to ensure that the Internet insurance products and services offered are consistent with the insurer's overall strategic and business plans and

the risk of offering such products and services is within the insurer's risk tolerance level;

(b) to take the necessary steps to identify, implement and monitor Internet insurance risks and implement effective security policies, procedures, limits and internal control systems to minimise risk and security exposure of the Internet insurance system from exploitation both from within and outside;

(c) to incorporate the security and privacy policies of Internet insurance into the insurer's overall business security programme and instil a corporate culture at all levels of staff that upholds security and confidentiality of information on the Internet insurance system at all times;

(d) to ensure that the system for Internet insurance is designed and operated in a manner that enables ease of timely implementation and compliance with all relevant laws, guidelines and consumer protection measures related to Internet insurance;

(e) to ensure that there are adequate expertise and resources to operate and maintain the Internet insurance system;

(f) to establish written effective channels of communication to ensure that the specific roles and responsibilities of employees are clear and transparent; the employees are fully aware of policies affecting their duties; there is clear delineation and segregation of roles, duties and responsibilities for managing Internet insurance risks in order to provide check and balance; and to inculcate and to draw up an employees' policy to exercise and uphold due care and diligence in carrying out their duties; and

(g) to establish and ensure that there are adequate, comprehensive and timely reports to the BOD for decision making on Internet insurance matters.

PART IV - RISK MANAGEMENT PRACTICES

16. EFFECTIVE RISK MANAGEMENT PRACTICES

16.1 The insurer should also put in place an effective risk management practices programme to identify, monitor, control and prevent or mitigate potential risks. The most effective programmes will customise hardware, software, procedures, controls and processes during the system development stage. Risk management practices, to be effective and relevant, should also be an ongoing dynamic process of identifying, measuring, monitoring and managing potential risk exposures in line with the insurer's risk appetites. Some aspects of the risk management practices to manage Internet insurance risks should cover the components listed in the following paragraphs.

17. STRATEGIC PLANNING AND FEASIBILITY ANALYSIS

17.1 The importance of incorporating strategic planning and feasibility analysis in the RMF cannot be overstated due to the significant investment, opportunities and risks in deploying the Internet capabilities. It should be an ongoing process, and changes in strategic planning should be reflected in the insurer's mission and objectives. The feasibility analysis will focus on the impact and whether specific proposals will fulfil specified objectives. Once deployed, each system or proposal should be subject to regular reviews to evaluate performance against current strategic plans and objectives, operating requirements and technological developments. Appropriate actions should be taken quickly to address deficiencies.

18. RISK PLANNING PROCESS

18.1 Effective planning will help the insurer to identify and quantify risks relating to the use of specific technology, maintain a prudent and manageable level of tolerable risk within its risk tolerance level and continuously assessing impact on performance and financial conditions compatible with the insurer's strategic goals and business strategies.

19. SELECTION OF TECHNOLOGY

19.1 The management should establish policies, procedures, and controls, training, testing, contingency planning and proper oversight of any outsourcing in the proper implementation of Internet insurance system. It should select and implement the right mix of Internet insurance technologies and products and services for the insurer and to ensure that they are properly installed.

20. MEASURING AND MONITORING RISK

20.1 The insurer should use an integrated approach in risk management to identify, measure, monitor and control all risks faced by insurers. This holistic approach is to avoid excessive risk-taking that may threaten the safety, soundness and viability of the insurer arising from the offering of products and services on the Internet. On the whole, the Internet insurance systems should be reviewed periodically to ensure that they continually address any new risks and to meet required performance standards.

21. SECURITY ARRANGEMENTS

21.1 In setting up a sound and secure insurance business on the Internet, the insurer must have a written security policy that draws up comprehensively and puts in place adequate measures to address both critical customer and the insurer's concerns of security and privacy in using the Internet insurance system.

21.2 The security policy must also be subject to regular reviews to ensure its relevance, appropriateness and effectiveness in addressing all identified and emerging issues on risks and confidentiality. The level of adequacy of security and types of security measures taken in the Internet insurance system will depend on the various types of products and services offered on the Internet and the degree of risks presented by each of these processes and the value of assets at risk. The security arrangements must manage the availability, integrity and authenticity of the insurer's information base. The security measures must also address not only risks from

outside, but also risks from within the insurer. All levels of staff must be made aware of and are required to strictly abide by the insurer's security policy.

21.3 Based on an evaluation of risks, costs and benefits, the insurer should strive for a combination of technological tools, better security management/controls and best practices to ensure acceptable security measures and arrangements are in place. The insurer should also have at its ready disposal, the budget and expenditure to continuously meet security needs appropriate to the magnitude and nature of the risks identified.

21.4 The Internet insurance system security arrangements should minimally achieve the following objectives:-

(a) **Data privacy and confidentiality**

The insurer should implement proper security precautions to ensure that data transfers are not monitored or read by any unauthorised parties and data storage systems are well protected. The customers must also have confidence that their information remains private and only accessible by legitimate and authorised parties.

(b) **Data integrity**

The insurer should undertake the necessary steps to ensure that data is not altered or modified during transmission anywhere from its point of origin to its destination. Data can also be compromised when residing within the insurer's data storage systems. As such, strong measures must be put in place to prevent unauthorised access to the insurer's central computer system and database.

(c) **Authentication**

The insurer should put in place authentication controls to establish the identities of all parties are who they say they are and a particular communication, transaction or access request is legitimate.

(d) **Non-repudiation**

The insurer should put in place measures to prohibit any parties from disputing the validity of, or refusing to acknowledge legitimate communications or transactions and ensure the legality and enforceability of transactions conducted on the Internet. Based on these measures, the insurer should state clearly online the procedures for valid and authentic electronic communications between the insurer and its customers. The agreements should also specify that the parties intend to be bound by communications that comply with these procedures.

(e) **Network and access controls**

The Internet-based insurance service seeks to provide connectivity to the wider world, as well as internal staff. Hence, the Internet insurance system should be designed to ensure that there are strong security measures to prevent unauthorised access attempts from within and outside to enter critical facilities such as the insurer's software applications, servers and operating systems and lead to, among others fraud in insurance transactions, destruction, alteration and/or theft of data, compromised data confidentiality, denial of service (systems failures), a damaged public image and the resulting financial and legal implications.

21.5 In this regard, to achieve the above security objectives in the Internet insurance system, as a minimal guide, the insurer should put in place a combination of critical technologies (or the latest available advanced security tools) and thorough and documented security procedures in accordance to the risk exposures and needs of its Internet insurance system as follows:-

(a) **Latest critical technologies available**

The insurer should continuously keep abreast and adopt the latest security measures available. Some of these latest critical technologies to address security concerns are as follows:-

(i) **Firewalls**

A firewall is a combination of hardware and software systems that determine the legitimacy of incoming and outgoing Internet traffic to ensure that only legitimate transmissions are permitted to engage the insurer's systems. The insurer should use firewalls to protect the insurer's internal computer network and all connection points between the internal computer network and the Internet according to the risk exposure assessment done by the insurer. The insurer should conduct periodic review and testing of operational soundness of firewalls as part of the insurer's security monitoring efforts. There should be clearly defined roles and responsibilities for maintaining and monitoring firewalls including that for the outsourcing vendor.

(ii) **Intrusion detection systems**

In addressing external attacks, it is imperative for the insurer to install strong intrusion detection devices to monitor network traffic on a real-time basis. Such a system must be capable of detecting and recording attempts to break into the insurer's computer system, with established procedures for handling such attempts. The intrusion detection system must itself be resistant to outside attacks and be capable of identifying and reporting deviations from normal processing. Adequate audit trail mechanisms should be in place to detect unauthorised intrusion or transactions. Internet-connected computers should also be running on an approved type of intrusion detection system (IDS), such as network IDS, host IDS or hybrid IDS that combine both solutions. This is to automatically monitor and immediately detect and provide alerts on suspicious activities, and allow insurers to promptly respond to any possible intrusions and take remedial measures such as isolating a system from an internal network or disabling certain user-IDs. A process for regular

update to incorporate new or updated attack characteristics should also be in place.

(iii) **Anti-virus or virus protection**

The insurer should establish an insurer-wide virus detection and prevention programme. This should include end-user policies, training and awareness programs, enforcement procedures, and virus detection tools such as anti-virus software to detect the presence or any known or potential computer viruses.

(iv) **Encryption**

The levels, types and strength of encryption technology adopted should be based on the sensitivity of data or information being transmitted such that unauthorised persons or systems are prevented from reading or compromising the actual information content. For instance, public key encryption can be deployed to encrypt the data, and the recipient's private key can be used to decrypt the data. Regardless of whether the insurer is using Secure Socket Layer (SSL) or Secure Electronic Transaction (SET) technology, all encryption keys must be protected with the most stringent controls. Where insurers act as Certificate Authorities for digital signatures, the customers must be educated about the importance of keeping the private keys confidential. A reporting mechanism must be put in place to enable customers to lodge reports about compromised keys.

(v) **Virtual private networks (VPN)**

A VPN uses firewall and encryption technology to create "tunnels" within a public switch network. All transmissions within the VPN are protected from unauthorised parties, while allowing the use of the public network infrastructure.

(vi) **Public key infrastructure (PKI)**

PKI is emerging as a reliable method to perform authentication on the Internet. A framework for securing applications is provided by a combination of the following elements:-

- Digital certificates

  These are electronic or online identifications, which verify that the identity of the certificate holder is who he/she is, or provide for secure web server thus providing confidence that a specific website is secure and genuine. An authorised Malaysian-licensed Certification Authority must issue these digital certificates; **and**

- Public key cryptography (PKC)

  The two principal operations in PKC provide for data encryption and the use of digital signatures.

The insurer may wish to use digital certificates and digital signatures as issued in accordance to the Digital Signature Act 1997 to address security issues such as secure genuine sites, non-repudiation and user authentication.

(vii) **Payment protocols**

The insurer should implement internationally accepted well-defined industry standards of payment protocol to provide a secure environment for online credit card payments. For this purpose, insurers are required to utilise MEPS “Payment Gateway” in respect of payments for any business transacted through the Internet.

(b) **Security procedures**

These could include usage of:-

(i) **User IDs and Passwords**

The insurer should provide User IDs and assign passwords or PINS for policy owners to control access to Internet insurance systems for conduct of transactions such as products purchase and/or renewal, claims processing and policy queries. Likewise, the staff of the insurer and the outsourcing vendor should also be assigned User IDs and passwords based on their access rights through their respective roles and responsibilities. The insurer should ensure the integrity of passwords by providing instructions to customers and staff on their proper use and protection. Facilities must be provided for the change of passwords on the website. Where necessary and critical, the use of passwords should be complemented with digital signatures issued as specified under the Digital Signature Act 1997 for user authentication and non-repudiation of transactions.

(ii) **Personal and policy details**

The insurer should require the policy owners to input personal details such as the NRIC numbers and policy numbers for user verification and authentication.

(iii) **Time stamping**

Successful policy statements for purchases and renewals should be time stamped to prevent backdating of documents and renewal records.

(iv) **Reconciliation**

The insurer should perform daily reconciliation of all successful transactions with the payment transaction statements provided by the relevant bank.

(v) **Segregation of roles and responsibilities**

This will provide for the check and balance to secure the internal corporate environment in the insurer and/or outsourcing vendor. The segregation of roles and responsibilities must be clearly documented for accountability and monitoring purposes.

(vi) **Audit trails**

The ability to trace transactions from the point of origin to the point of destination will enable the insurer to verify specific transactions and also facilitate proof of transactions to address the issue of repudiation of legitimate transactions by customers and monitor activities of both the internal staff and the vendor's staff.

(vii) **Testing**

The insurer should place a strong emphasis on using monitoring tools to continuously identify vulnerabilities and in a real-time mode, detect possible intrusions from external and internal parties. In this regard, the insurer is required to conduct penetration testing to identify, isolate, and confirm possible flaws in the design and implementation of passwords, firewalls, encryption and other security controls. In simulating the probable actions of unauthorised and authorised users, the insurer is able to evaluate the continuous effectiveness of security controls. The testing should be conducted by an objective, qualified internal or external source prior to the introduction of Internet insurance and at least once a year or whenever substantial changes are made to the Internet insurance systems.

22. INCIDENT RESPONSE AND PREPAREDNESS

22.1 The insurer should have an incident response team or preparedness plan to provide a platform from which an insurer can respond quickly to a problem situation. This is critical in an Internet-enabled environment where the technology employed offers speed, sophistication and access to many anonymous users who may have illegitimate/malicious intent in accessing these systems. Furthermore, since the systems are interdependent, a single problem may have impact on several areas including product management, marketing and customer service and operations. The composition of a response team, such as the number, expertise and department will depend on the level and complexity of the Internet insurance activity.

23. CONTINGENCY AND BUSINESS RESUMPTION PLANS

23.1 The BOD should approve such plans before the launch of the insurer's Internet insurance activities. A contingency and business resumption plan is vital to ensure continuity of insurance business and the provision of good customer services. It should include data recovery, alternate data processing capabilities, order priority for resumption of business applications and processes, emergency staffing and a public relations and outreach strategy to respond promptly to customer and media reaction to system failure or unauthorised intrusions. The backup systems should be fully maintained and tested on a regular basis to upkeep and minimise risk of system failures and unauthorised intrusions. It is expected that the security and internal controls at the backup location should be as comprehensive and sophisticated as those at the primary site.

24. OBJECTIVE REVIEW AND AUDIT REQUIREMENTS

24.1 The management should undertake an objective review of Internet insurance systems to identify and quantify risks, to establish adequacy of internal controls and procedures, policies and processes and detect possible weaknesses in the insurer's risk management system. This should include a post implementation review to

assess the Internet insurance systems' operational performance. The relative success of the Internet insurance systems should be gauged by comparing planned and actual costs, benefits and development time. If the planned objectives do not materialise, reasons should be reviewed and documented in a post implementation evaluation report that should be presented to senior management. The review may be conducted by internal audit, external audit or other appropriately qualified professional entities. Appropriate policies, procedures and standards should be developed and practised where necessary to maintain a tight risk control framework.

25. STAFF AND EXPERTISE REQUIREMENTS

25.1 The management should identify the staffing and training needs to support Internet insurance activities in areas including system development, operations, and security implementation and customer support. The staffing plan should incorporate clear and written specifications of roles and responsibilities to ensure that there is no potential conflict in tasks assigned and that there is check and balance. There should also be sufficient relevant resources at all times including the availability of immediate staff when critical staff leaves or when the usage of the system exceeds expectations.

26. OUTSOURCING

26.1 The outsourcing of the Internet insurance system to vendors should be read in conjunction with relevant guidelines/circulars issued by the Bank with regard to outsourcing by insurers. Any outsourcing of information technology services that relates to Internet insurance should also abide by the following:-

(a) the written approval of the BOD has been obtained;

(b) the control and flexibility in all strategic and material decisions on the operations and processes of the insurer remains with the insurer;

(c) the insurer is fully aware and is able to manage the risks associated with the relationship with the vendor and the appropriate oversight framework is in place to monitor the outsourcing vendor's controls, condition and performance;

(d) the insurer 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 including regular reporting by the vendor to the insurer of status of work done;

(e) the external and internal auditors of the insurer have access to the books of the outsourcing vendor and perform audits. Any weaknesses highlighted in audit reports must be well-documented and promptly rectified especially where it impacts the integrity of the internal controls of the insurer;

(f) the ownership and control of the insurer's records remains with the insurer and the service provider or software vendor is to provide the insurer with a written undertaking on its compliance with secrecy of customers' and the insurer's information; and

(g) the vendor is also to abide by any data protection legislation that is in effect.

27. REPORT ON SECURITY BREACHES, SYSTEM DOWNTIME AND DEGRADATION IN SYSTEM PERFORMANCE

27.1 The staff of the insurer and any outsourcing vendor are required to report all security breaches promptly to management. Material security breaches, system downtime and degradation in system performance that critically affects the insurer should also be reported to Pengarah, Jabatan Penyeliaan IT dan IKP, Bank Negara Malaysia as follows:-

(a) an initial report to BNM should be made via telephone immediately upon detection by providing 'initial information/observation; and

(b) a formal report should be made within two days from the date of detection, and contain, among others, the date and time the incident was detected, brief description/information of the problem and actions taken to date. The report should also contain the name of person to be contacted for further enquiries and his/her phone number, fax number and e-mail address.

27.2 The above requirements should be stated explicitly in the insurer's security policy. The insurer should also establish procedures for proper recording of occurrence of such incidents.

28. PRODUCT INFORMATION AND TRANSPARENCY

28.1 The insurer is required to ensure that all information including those on products and services offered, and the computation of premium on the Internet are fairly and accurately disclosed. All products and services must abide by the relevant legal and administrative provision requirements.

29. CUSTOMER EDUCATION, PROTECTION AND PRIVACY ISSUES

29.1 The issues of customer education, customer protection and privacy take on an even greater significance in an Internet-enabled insurance environment. As such, the insurer should put prominently on the website, any statements relating to these issues to facilitate and maintain a sound environment for customers to conduct insurance transactions on the Internet with confidence:-

(a) **Customer education**

The insurer should consider having a web page to educate and inform its customers on the conduct of its insurance business on the Internet. This would include educating customers of their rights and responsibilities, on how customers should take conscientious efforts to protect their own privacy on the Internet and to inform of the roles and responsibilities of the insurer on the Internet, including the insurer's communication particulars. The customers are also required to have agreed with the insurer's terms and conditions before undertaking Internet insurance transactions.

(b) **Client Charter**

Every insurer offering products and services on the Internet is required to provide a Client Charter. The Client Charter should minimally state the insurer's commitment to provide safe and secure operations, maintaining customer privacy, providing reliable and quality services, providing comprehensive and transparency in product information and services and providing prompt response to enquiries and complaints.

(c) **Internet Privacy Policy Statement**

The very nature of the Internet potentially enables the vast collection, mining and manipulation of customer information. The Bank considers the privacy of such customer's information to be paramount in maintaining public confidence and ultimately a sound operating environment in the insurance industry. The insurer should maintain responsible Internet privacy policy practices, ensure that the insurer's staff observe these policies as part of the insurer's corporate culture and to keep close tab on and ensure compliance with the developments in areas concerning customer protection. The privacy policy statement should be clear and easily understood by customers. The icons for the privacy statement must be highly visible where customers can easily locate it and the insurer should minimally prompt customers to refer to this statement where the individual's information is collected.

30. INSPECTION BY BANK NEGARA MALAYSIA

30.1 The web servers, books and records should be maintained in Malaysia for the Bank's inspection.

PART V - WITHDRAWAL OF GUIDELINES/CIRCULARS

31 With the issuance of these consolidated Guidelines, the previous Guidelines and circulars relating to internet insurance as stated below are deemed withdrawn:-

Guidelines/ Circulars	Title	Date of Issuance
JPI/GPI 26	Guidelines on Internet Insurance by Insurers	18 October 2000
JPI: 7/2000	Insurans Internet	28 April 2000
JPI: 19/2003	Internet Insurance	24 September 2003
JPI: 4/2004	Internet Insurance	7 February 2004

PART VI - APPENDICES

APPENDIX I

SUBMISSION PARTICULARS

As a guide to the submission and processing of applications to seek the Bank's approval to conduct Internet insurance, besides observing the Guidelines, the insurer is also required to provide the following information:-

1. the products and services offered on the Internet and the process flow;

2. the Internet insurance security arrangements and policy; and

3. the attestation of the Chairman, to represent the BOD of the insurer, that the insurer has observed the Guidelines for and stands ready to provide Internet insurance, as attached in **Appendix II**.

APPENDIX II

ATTESTATION BY THE CHAIRMAN OF THE BOARD THAT THE INSURER IS READY TO PROVIDE INTERNET INSURANCE

Name of Insurer ……

As Chairman of the board of directors of [name of Insurer], I confirm that:

(i) internet insurance is consistent with the insurer's strategic and business plans;

(ii) the board of directors and senior management understand and are ready to assume the roles and responsibilities stated in the Guidelines on Internet Insurance and are also apprised of all relevant provisions in the Insurance Act and the Insurance Regulations and other relevant legislations, guidelines and codes of conduct;

(iii) risk management process related to Internet insurance is subject to appropriate oversight by the board of directors and senior management;

(iv) appropriate security measures to address Internet insurance security concerns are in place;

(v) customer support service and education related to Internet insurance are in place;

(vi) performance monitoring of Internet insurance products, services, delivery channels and processes has been established;

(vii) internet insurance is included in the contingency and business resumption plans;

(viii) there are adequate resources to support the offering of Internet insurance business; and

(ix) the systems, procedures, security measures, etc. relevant to sound operations of Internet insurance will constantly be reviewed to keep up with the latest changes.

Signature : ……

Name : ……

Date : ……..……..