Information Technology Security Policy of Insurance Information Bureau (IIB)

1.0 Policy Statement

Insurance Information Bureau is constituted by Insurance Regulatory and Development Authority (IRDA)

- Maintains electronic information resources which are essential to performing Data Center functions.
- Similar to any other capital resources owned by the IRDA, these resources are to be viewed as valuable assets over which IRDA has both rights and obligations to manage, protect, secure, and control.
- IIB employees, Insurers and other stake holders are expected to utilize these resources for appropriate purposes, protect access to them, and control them appropriately.
- Examples of information resources include, but are not limited to, computer systems, network systems, software and data.

2.0 Purpose

This policy sets forth the mechanisms by which data stored on IIB owned computing systems and utilized by IIB employees and insurers is secured and protected. This policy is adopted and promoted in order that:

1. IIB can consistently maintain data integrity and accuracy.
2. IIB can assure that authorized insurers and other stake holders have timely and reliable access to necessary data.
3. IIB can assure that unauthorized persons are denied access to computing resources or other means to retrieve, modify or transfer data.
4. IIB can comply with the Information Technology Act, 2000 (as amended).

Every employee, user and stakeholders of IIB data must be aware of these risks, and act in a way to protect the information resources of IIB.

3.0 Scope

This policy applies to all persons associated with IIB, including, but not limited to

- Employees
- Insurers
- Vendors
- temporary staff

This policy applies to all IIB owned information technology hardware and its software, including, but not limited to, desktop workstations, servers and other available resources, such as

- servers
- personal computers and Laptops
- network systems
- access card systems
- other technology hardware

The policy applies to all IIB data, and reports derived from IIB data; and it applies to all programs utilizing IIB operational data.

4.0 User Identifications and Passwords

No one should access IIB information systems without an authorized user identification code (userid) and password. Receiving a userid requires approval of the individual(s) responsible for the system in question. Userids may be revoked or disabled to protect the system at any time. Userids will be revoked if the employee or other users etc terminates the relationship with the IIB. Inactive userids are temporarily disabled until continued need can be established.

5.0 Policy Awareness

Every employee, Insurer and other users of IIBôs resources should have access to a copy of this policy. All new entrants should be made aware of the importance of information systems security and their responsibilities in the process. All effort should be made to include this policy in existing communication mechanisms for policy dissemination.

All employees must be made aware of the Information Security Policy Prior to userids being issued; the user should be notified of the security practices and the policy of IIB.

6.0 Access to Equipment

Only authorized persons whose work requires will be allowed access to information systems resources. All information systems resources will be protected against fire, water, physical damage and theft. The appropriate protection will be selected from among physical barriers, environmental detection and protection, insurance, and other risk management techniques.

7.0 Access to Data

All data and program files on IIB information systems will be protected against unauthorized changes. Sensitive data and program files will be protected against unauthorized reading and copying. IIB information systems shall be programmed to control which userids can read and/or write to any given file.

Every file shall be associated with an owner. The owner of each file is responsible for specifying whether the file is sensitive and which userids should be allowed to read and/or write to it.

All programs will be designed in such a manner that a log of the usage and amendments, if any will be automatically retained in the log files.

8.0 Violations

Violations of this policy will be treated as severe offence and will attract suitable action as decided by IIB.

9.0 Related Policies and Procedures

The IIB Data sharing Policy and any other policy implemented by IIB in addition to the policies mentioned below complement this policy and are considered instrumental in completing this policy.

I. Backup Policy
II. Password Policy

10.0 Revisions

As an ongoing document, the IIB Information Security Policy will be reviewed periodically by IIB.

11.0 Endorsements

This policy has been approved and endorsed by the IIB Board.