With the increasing use of new emerging technologies and growing reliability on internet technologies in the global world of technology (IT), Information and Cyber Security has become critical to today's organisations. The nature of cyber attacks have been changing drastically with the sophisticated technologies emerging in recent days. Today's technology is no longer limited to simple hardware & software. More easier & seamless ways of technologies such as Internet of Things (IoT), Data Analytics, Block chains and Mobile computing rapidly developed giving more scope for effective and holistic implementation of Information and Cyber Security in organizations.

The three basic principles of Security i.e Confidentiality, Integrity and Availability has become more vital with the increase of sophisticated attacks happening in recent days. It is therefore essential for all organizations to maintain effective security measures and controls against the sophisticated cyber attacks.

Information and Cyber Security policy defines necessary procedures, controls and guidelines for establishing, implementing, maintaining and continually improving information security system within the organization.

**Information & Cyber Security Policy Statement of BDL**

*"To protect and safeguard critical information and information processing assets, in order to ensure secure provisioning of services by maintaining confidentiality, integrity and availability of data. This includes (but not limited to) electronic information on PC's, servers, workstations, laptops, networking devices, portable media etc."*

BDL prepared a detailed Information & Cyber Security Policy Document and put in to use for its internal purpose which constitutes the following contents

1.0    Organization Structure of Information & Cyber Security

2.0    Key Roles & Responsibilities

3.0    Human Resource Management Policy

4.0    Asset Management and Holders Responsibility

5.0    Physical & Equipment Security

6.0    Network Design & Security

7.0    Mobile Security

8.0    Security in Support Processes

9.0    Secure Configuration and Access Control

10.0    Monitoring the Assets

11.0    Cryptographic Controls

12.0    Operational Control

13.0    Handling of Storage and Removable Media

14.0    E-mail Policy

15.0    Internet Policy

16.0    Embedded Software

17.0    Security Audit

18.0    Cyber Crisis and Incident Management

19.0    User Education, Training & Cyber Security Awareness

20.0     Business Continuity Plan (BCP) And Business Continuity Management (BCM)

21.0    Risk Management

The detailed Information Security Policy document is placed on Local Area Network (LAN) for reference and compliance of users.

The steps taken towards Cyber Eco System in BDL are in compliance with various guidelines issued by the Government Agencies.