

## **BMD SCEURITIES LIMITED**

### **INFORMATION SECURITY POLICY**

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31-12-2024
Policy Approved by	Board of Directors
Policy approved on	28-04-2025

**Version - 1.2**

# BMD SECURITIES LIMITED

## INFORMATION SECURITY POLICY

Circular: Ref: SMD/INFORMATION SECURITY/001/2018 dated December-03, 2018

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31-12-2014
Policy Approved by	Board of Directors
Policy approved on	28-01-2015

Version - 1.2



## **Purpose**

The purpose of this Policy is to safeguard information belonging to the Company and its stakeholder (third parties, clients or customers and the general public), within a secure environment.

This Policy informs the Company's staff, and other external Vendors entitled to use Company facilities, of the principles governing the holding, use and disposal of information.

## **It is the goal of the Company that**

- Information will be protected against unauthorised access or misuse.
- Confidentiality of information will be secured.
- Integrity of information will be maintained.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical, logical, environmental and communications security will be maintained.
- Infringement of this Policy may result in disciplinary action or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to the Director of ICT Systems and investigated through the appropriate management channel.

## **Information relates to**

- Electronic information systems (software, computers, and peripherals) owned by the Company whether deployed or accessed on or off campus.
- The Company's computer network used either directly or indirectly.
- Hardware, software and data owned by the Company.
- Paper-based materials.
- Electronic recording devices (video, audio, CCTV systems).

## **The Policy**

The Company requires all users to exercise a duty of care in relation to the operation and use of its information systems.

## **Authorised users of information systems**

- With the exception of information published for public consumption, all users of Company information systems must be formally authorised by appointment as a member of staff, or by other process specifically authorised by the designated officer. Authorised users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person. The "Network password policy" describes these principles in greater detail.

- Authorised users will pay due care and attention to protect Company information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:
  - permission of the information owner
  - the risks associated with loss or falling into the wrong hands
  - How the information will be secured during transport and at its destination.

### **Acceptable use of information systems**

- Use of the Company's information systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people. The detail of acceptable use in specific areas may be found in the list of subsidiary policies.

### **Information System Owners**

- Designated Officer/Chief Technology Officer/Directors who are responsible for information systems are required to ensure that:
  - Systems are adequately protected from unauthorised access.
  - Systems are secured against theft and damage to a level that is cost-effective.
  - Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
  - Electronic data can be recovered in the event of loss of the primary source. I.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
  - Data is maintained with a high degree of accuracy.
  - Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
  - Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
  - Any third parties entrusted with Company data understand their responsibilities with respect to maintaining its security.

### **Personal Information**

- Authorised users of information systems are not given rights of privacy in relation to their use of Company information systems. Duly authorised officers of the Company may access or monitor personal data contained in any Company information system (mailboxes, web access logs, file- store etc.).
- Individuals in breach of this policy are subject to disciplinary procedures at the instigation of the Designated Officer with responsibility for the relevant information system, including referral to the Police where appropriate.
- The Company will take legal action to ensure that its information systems are not used by unauthorised persons.




## Ownership

- The Designated Officer of ICT Systems has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.
- Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

For BMD Securities Ltd

A circular stamp of BMD Securities Ltd, Kolkata, with a signature over it. The stamp contains the text "BMD SECURITIES LTD" around the perimeter and "KOLKATA" in the center. A handwritten signature, "Utpal Mallick", is written across the stamp.

Utpal Mallick

CISO

Dated: - 30-04-2025

Ownership

The Board of Directors of the Company has the responsibility for maintaining the policy and providing guidance and supervision for the implementation of the policy. The Board of Directors is also responsible for the implementation of the policy. The Board of Directors is also responsible for the implementation of the policy.

Changes in the policy will be adopted as and when required by the company and is binding on all the shareholders and Directors of the Company.

For Board resolution

*[Signature]*

Chairman

CEO

Date: 30-04-2025