Annexure - A

CERTIFIED TRUE COPY OF THE RESOLUTION PASSED IN THE MEETING OF THE BOARD OF DIRECTORS OF PRISM INTERNATIONAL PRIVATE LIMITED HELD ON THURSDAY, JUNE 29, 2023 AT 206, SOUTHERN PARK, SAKET DISTRICT CENTRE, SAKET, NEW DELHI – 110 017.

APPROVAL OF MODIFICATION IN INFORMATION TECHNOLOGY POLICY/ INFORMATION SYSTEM POLICY OF THE COMPANY

"RESOLVED THAT pursuant to the provisions of Master Direction DNBS.PPD. No. 04/66.15.001/2016-17 dated June 08, 2017, the Information Technology/Information System Policy, be and hereby modified by inserting following clause after the clause "Information Security" in the policy:

Cyber Security

PIPL takes effective measures to prevent cyber-attacks and to promptly detect any cyber intrusions to respond / recover / contain the fall out. Among other things, PIPL takes necessary preventive and corrective measures in addressing various types of cyber threats which include denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, and password related frauds."

For **PRISM INTERNATIONAL PRIVATE LIMITED**

Ishaan Gupta

(Ishaan Gupta)
Director
DIN:05298583

PRISM INTERNATIONAL PRIVATE LIMITED

INFORMATION TECHNOLOGY / INFORMATION SYSTEM POLICY

(updated upto June 29, 2023)

INTRODUCTION

The Prism International Private Limited (hereinafter referred to as the Company or PIPL) has adopted an Information Technology/Information System Policy, in compliance with the RBI's has issued Master Direction DNBS.PPD. No. 04/66.15.001/2016-17 dated June 08, 2017. The Master Direction issued is mainly in respect of Information Technology Framework for the NBFC Sector. These Directions on IT Framework for the NBFC sector that are expected to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers.

SECURITY AND PASSWORD POLICY

1. For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and provide appropriate access through key lock.

2. All security and safety of all portable technology, such as laptop, notepads, iPad etc., will be the responsibility of the employee to whom it's issued.

3. In the event of loss or damage, the board will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

4. Every employee will be issued with a unique identification code to access the business technology.

5. Each password is to be alphanumeric and is not to be shared with any employee within the business.

6. Mr. Ishaan Gupta, Director of the Company will be responsible for the issuing of the identification code and initial password for all employees.

7. Where an employee forgets the password or is 'locked out' after three attempts, then Mr. Ishaan Gupta, Director of the Company is authorised to reissue a new initial password.

SOFTWARE INSTALLATION AND USAGE

1. All software must be appropriately installed and registered with the owner, wherever applicable, by the designated professional.

2. Unauthorised software is prohibited from being used in the business. This includes the use of software owned by an employee or bringing software from home and loading it onto the business's computer hardware.

3. The unauthorised duplicating, acquiring or use of software copies is prohibited.

4. The Company has adequate IT Systems to file the regulatory returns with the RBI (COSMOS Returns);

5. Based on the size and operations, the Company has adequate IT Systems to provide the reports in the form of excel charts etc. to the top management, summarising the financial position of the Company including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc. Further, the Company has in place Management information systems policy in order to generate and provide timely reports to the top management of the Company.

6. As and when the size and operations of the Company increases, the Company shall upgrade its IT systems

ELECTRONIC FUNDS TRANSFER (EFT)

1. All EFT payments and receipts must adhere to all finance policies.

2. EFT payments must have the appropriate authorisation for maker and checker.

3. EFT payments must be appropriately recorded.

4. For good control over EFT payments, ensure that the persons authorising the payments and making the payment are not the same person.

INFORMATION SECURITY

1. All data is to be backed-up. In order to ensure the validity and integrity of backup, the Company shall carry out periodic tests.

2. It is the responsibility of the user to ensure that data back-ups are conducted daily and the backed up data is kept on network server + mirrored second hard drive inside each computer.

3. All technology that has internet access must have anti-virus software installed. It is the responsibility of the user and designated professionals to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

4. To make every reasonable effort to ensure that the Company's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected.

5. All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements.

CYBER SECURITY

PIPL takes effective measures to prevent cyber-attacks and to promptly detect any cyber intrusions to respond / recover / contain the fall out. Among other things, PIPL takes necessary preventive and corrective measures in addressing various types of cyber threats which include denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, and password related frauds.

PERSONAL MOBILE DEVICES FOR BUSINESS USE

Personal mobile devices can only be used for email access, business internet access, business telephone calls etc.

USER ROLE

1. All computer software copyrights and terms of all software licences will be followed by all employees of the business.

2. Where licensing states limited usage, then it is the responsibility of the user to ensure these terms are followed.

SYSTEM FAILURE

1. Where there is failure of any of the business's hardware, this must be referred to designate IT Professionals immediately.

2. In the event that the business's information technology is compromised by software virus or such breaches are to be reported to IT Professionals immediately.

IS AUDIT

The IS/IT System will be audited annually as per the RBI Master Direction DNBS.PPD.No.04/66.15.001/2016-17 dated June 8, 2017, as and when applicable to the Company.

BACKUP

1. Weekly backups are taken manually on external storage media.
2. Each backup set is labelled for identification. The format of label is as follows: Prism<date><Month><Year>_<Time> e.g.: **Prims010120_10am**