INTERNAL POLICY & PROCEDURES

This policy and procedures document lists out various terms of operation and client service standards laid out by the management of AGROY. All employees, clients and associates of AGROY shall deal in securities as per the guidelines specified in this master policy documents. This Master Policy Document is revised from time to time and the latest policy document in force is available on the website of Agroy.

TABLE OF CONTENTS

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

IMPORTANT NOTE
We do not accept cash from clients under any circumstances
We do not offer portfolio management services and do not guarantee any returns on investment to clients
We do undertake PRO trading in our own account.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

CLIENT DEALING RELATED

1. Client Registration:

Following points are to be ensured at time of client registration:

i. The client holds a valid PAN card (the same should be verified from Income Tax Database)
ii. Ensure the validity of the address and bank account of the client (the same should not be 2 month old at time of opening the account)
iii. Conduct an in-person verification to establish genuine existence of the client (the same should be done by an employee of the Company or its Authorised Person)
iv. Trading is activated for the client only on the exchange / segment specifically opted by the client and not on any other exchange / segment at the discretion of Agroy. (the opted exchange / segment must be clearly marked on the KYC form and countersigned by the client)
v. Sufficient information with respect of financial status and income level of the client is obtained specifically for trading in F&O Segment. (Latest ITR copy or 6 months bank statement must be obtained every year for trading in F&O)
vi. KYC Form should be completely filled and signed by the client
vii. Email-ID and mobile number of the client should be obtained for sending contract notes and trade confirmations
viii. A unique client code should be allotted to every client and the same should be intimated to the exchange
ix. A copy of the KYC along with the Mandatory Section of KYC Form (containing Rights & Obligations, RDD, Guidance Note, Policies & Procedures and Tariff Sheet) must be delivered to the client within 15 days of the opening of the account.
x. All new clients must be introduced by either an existing client or an employee of the Company or its Authorised Person (such introducer must counter sign the KYC form)
xi. A welcome telephone call must be made to the client from the Head Office and various details of the client including PAN, date of birth, email ID and Mobile Number should be verified (Such calls shall be made from recorded telephone lines and a log of such calls should be kept).
xii. A welcome kit which includes client details, brokerage and taxes charged, demat client master, demat delivery instruction booklet, copy of KYC form, along with account operating instructions and guidelines shall be sent to every new client within 7 days of activation of the account.

2. Updation of Client Details

For keeping the client details with respect to address, telephone number, email ID, bank account, demat account, PAN, etc., up-to-date, following is ensured:

i. A KYC updation form is sent to all the client with every quarterly statement of funds and securities so that clients can submit their latest details to the company
ii. A KYC Updation form is readily available on the website so that clients can download and send the same to the company anytime they wish to change any of their details

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

iii. The web-based accounts interface of the company prominently displays the client details recorded with the company. In case of any changes or errors, the client can report the same to the company immediately.

iv. All bounced emails and document posts returned are recorded and a telephone call is made to such clients to ascertain the reason of bounce / return. In case of change of email id / postal address, the client is asked to furnish KYC updation form.

v. Financial information like 6 months bank statement or latest ITR or salary slip etc is collected every year from all the clients trading in F&O segment. In the month of April every year, all such F&O accounts are temporarily suspended where latest financial details have not been received from the client.

vi. All payout cheques carry the bank account details of the client so that the cheques cannot be deposited by the client in any other account. For updation of bank account details, the client has to submit the KYC updation form along with a cancelled cheque of the new bank account.

TRADE & RMS RELATED

1. Refusal of orders for penny / illiquid stock

Agroy may from time to time limit (quantity/value) / refuse orders in one or more securities due to various reasons including market liquidity, value of security(ies), the order being for securities which are not in the permitted list of Agroy / exchange(s) / SEBI.

Provided further that stock broker may require compulsory settlement / advance payment of expected settlement value/ delivery of securities for settlement prior to acceptance / placement of order(s) as well.

Provided further, that stock broker may require reconfirmation of orders, which are larger than that specified by Agroy's risk management, and that Agroy has the discretion to reject the execution of such orders based on its risk perception.

2. Setting up client's exposure limits and conditions under which a client may not be allowed to take further position or the broker may close the existing position of a client

Agroy may from time to time impose and vary limits on the orders that the client can place through Agroy's trading system (including exposure limits, turnover limits, limits as to the number, value and/or kind of securities in respect of which orders can be placed etc.).

Agroy may need to vary or reduce the limits or impose new limits urgently on the basis of Agroy's risk perception and other factors considered relevant by Agroy including but not limited to limits on account of exchange/ SEBI directions/limits (such as broker level/ market level limits in security specific / volume specific exposures etc.), and Agroy may be unable to inform the client of such variation, reduction or imposition in advance. Agroy shall not be responsible for such variation, reduction or imposition or the client's inability to route any order through Agroy's trading system on account of any such variation, reduction or imposition of limits.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Agroy may at any time, at its sole discretion and without prior notice, prohibit or restrict the client's ability to place orders or trade in securities through Agroy, or it may subject any order placed by the client to a review before its entry into the trading systems and may refuse to execute / allow execution of orders due to but not limited to the reason of lack of margin / securities or the order being outside the limits set by stock broker / exchange/ SEBI and any other reasons which Agroy may deem appropriate in the circumstances. The losses, if any on account of such refusal or due to delay caused by such review, shall be borne exclusively by the client alone. Agroy is required only to communicate / advise the parameters for the calculation of the margin / security requirements as rate(s) / percentage(s) of the dealings, through anyone or more means or methods such as post / speed post / courier / registered post / registered A.D / facsimile / telegram / cable / e-mail / voice mails / telephone (telephone includes such devices as mobile phones etc.) including SMS on the mobile phone or any other similar device; by messaging on the computer screen of the client's computer; by informing the client through employees / agents of Agroy; by publishing / displaying it on the website of Agroy / making it available as a download from the website of Agroy; by displaying it on the notice board of the branch / office through which the client trades or if the circumstances, so require, by radio broadcast / television broadcast / newspapers advertisements etc; or any other suitable or applicable mode or manner. The client agrees that the postal department / the courier company /newspaper company and the e-mail / voice mail service provider and such other service providers shall be the agent of the client and the delivery shall be complete when communication is given to the postal department / the courier company / the e-mail/voice mail service provider, etc. by Agroy.

The client shall monitor his / her / its position (dealings / trades and valuation of security) on his / her / its own and provide the required / deficit margin / security forthwith as required from time to time whether or not any margin call or such other separate communication to that effect is sent by Agroy to the client and /or whether or not such communication is received by the client.

The client is not entitled to trade without adequate margin / security and that it shall be his / her / its responsibility to ascertain beforehand the margin / security requirements for his/ her /its orders / trades / deals and to ensure that the required margin / security is made available to Agroy in such form and manner as may be required by Agroy. If the client's order is executed despite a shortfall in the available margin, the client, shall, whether or not Agroy intimates such shortfall in the margin to the client, make up the shortfall suo moto immediately. The client shall be responsible for all orders (including any orders that may be executed without the required margin in the client's account) & / or any claim /loss/ damage arising out of the non availability /shortage of margin /security required by Agroy & / or exchange & / or SEBI. Agroy is entitled to vary the form (i.e. the replacement of the margin / security in one form with the margin / security in any other form, say, in the form of money instead of shares) & / or quantum & / or percentage of the margin & / or security required to be deposited / made available, from time to time.

Agroy is entitled to disable / freeze the account & / or trading facility / any other service / facility, if, in the opinion of Agroy, the client has committed a crime / fraud or has acted in contradiction of this agreement or / is likely to evade / violate any laws, rules, regulations, directions of a lawful authority whether Indian or foreign or if Agroy so apprehends.

3. Client Funding Violations

As per Circular issued by NSE (NSE/INSP/20638) dated April 26, 2012, all debit balances in any client account must be cleared within 7 days of trade date. In case it is not settled within 7 days, then the client should not be provided additional exposure to trade.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Broker's have been instructed to close out the stock (sell the securities) of the client by the 7th day, in case the debit balance is not cleared within 7 days of trade date.
Client's stock / collateral cannot be submitted to Exchange as Margin in F&O. In case any broker allows any client to trade in F&O against stock as margin, then this will be considered as client funding and interest is chargeable on the same.

4. The right to sell clients' securities or close clients' positions, on account of non-payment of client's dues

Agroy maintains centralized banking and securities handling processes and related banking and depository accounts at designated place. The client shall ensure timely availability of funds/securities in designated form and manner at designated time and in designated bank and depository account(s) at designated place, for meeting his/her/its pay in obligation of funds and securities.

Agroy shall not be responsible for any claim/loss/damage arising out of non availability/short availability of funds/securities by the client in the designated account(s) of Agroy for meeting the pay in obligation of either funds or securities. If the client gives orders / trades in the anticipation of the required securities being available subsequently for pay in through anticipated payout from the exchange or through borrowings or any off market delivery(s) or market delivery(s) and if such anticipated availability does not materialize in actual availability of securities / funds for pay in for any reason whatsoever including but not limited to any delays / shortages at the exchange or stock broker level / non release of margin by Agroy etc., the losses which may occur to the client as a consequence of such shortages in any manner such as on account of auctions / square off / closing outs etc., shall be solely to the account of the client and the client agrees not to hold Agroy responsible for the same in any form or manner whatsoever.

Where the margin /security is made available by way of securities or any other property, Agroy is empowered to decline its acceptance as margin / security & / or to accept it at such reduced value as Agroy may deem fit by applying haircuts or by valuing it by marking it to market or by any other method as Agroy may deem fit in its absolute discretion.

Agroy has the right to cancel all pending orders and to sell/close/liquidate all open positions/ securities / shares at the pre-defined square off time or when Mark to Market (M-T-M) percentage reaches or crosses stipulated margin percentage mentioned on the website, whichever is earlier. Agroy will have sole discretion to decide referred stipulated margin percentage depending upon the market condition. In the event of such square off, the client agrees to bear all the losses based on actual executed prices. In case open position (Le. short/long) gets converted into delivery due to non square off because of any reason whatsoever, the client agrees to provide securities/funds to fulfill the payin obligation failing which the client will have to face auctions or internal close outs; in addition to this the client will have to pay penalties and charges levied by exchange in actual and losses, if any. Without prejudice to the foregoing, the client shall also be solely liable for all and any penalties and charges levied by the exchange(s).

Agroy is entitled to prescribe the date and time by which the margin / security is to be made available and Agroy may refuse to accept any payments in any form after such deadline for margin / security expires. Notwithstanding anything to the contrary in the agreement or elsewhere, if the client fails to maintain or provide the required margin/fund / security or to meet the funds/margins/ securities pay in obligations for the orders / trades / deals of the client within the prescribed time and form, Agroy shall

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

have the right without any further notice or communication to the client to take any one or more of the following steps:

i. To withhold any payout of funds / securities.
ii. To withhold / disable the trading / dealing facility to the client.
iii. To liquidate one or more security(s) of the client by sellingthe same in such manner and at such rate which Agroy may deem fit in its absolute discretion. It is agreed and understood by the client that securities here includes securities which are pending delivery / receipt.
iv. To liquidate / square off partially or fully the position of sale & / or purchase in anyone or more securities / contracts in such manner and at such rate which Agroy may decide in its absolute discretion.
v. To take any other steps which in the given circumstances, Agroy may deem fit.

The client agrees that the loss(s) if any, on account of anyone or more steps as enumerated herein above being taken by Agroy, shall be borne exclusively by the client alone and agrees not to question the reasonableness, requirements, timing, manner, form, pricing etc., which are chosen by Agroy.

5. Order Punching Errors and Client Code Modification

This Error Policy has been made in accordance with the SEBI directives and NSE Circulars NSE/INVG/18281 dated Jul 5, 2011, NSE/INVG/18484 dated Jul 29, 2011 and NSE/INVG/18716 dated Aug 29, 2011.
As per the SEBI directive, client code modification and order entry errors shall be rectified only in following cases:

a) Only genuine order entry errors where the wrong client code / client name is very similar to the actual client code / client name
b) Only genuine order entry errors where the wrong client is a relative of the actual client

The procedure to be followed for rectification of the above orders entry errors is as follows:

a) All such errors along with the reason of error must be recorded in a Errors / Modification Register maintained at HO
b) Such errors to be rectified only subsequent to authorisation by a Director or Compliance Officer of the Company
c) An error code with UCI as 'ERROR' to be uploaded on the Exchange. Such error code is to be used to rectify the order entry errors
d) All erroneous trades to be modified using the facility provided by the exchange by transfer from the wrong client code to the error code. And subsequently such trades to be squared off / liquidated in the error code.
e) Direct transfer of trade by modification of client code from wrong code to correct code shall not be allowed under any circumstances
f) Upon liquidation of the erroneous trade in the error code, the actual correct code must be done as a fresh trade in the correct client code
g) The details of rectification, i.e the liquidation trade in error code and the fresh trade in actual code must be recorded in the error / modification register maintained at HO.

ACCOUNTS & SETTLEMENT RELATED

1. Applicable Brokerage Rate

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

The applicable rate of brokerage may differ from client to client and from time to time. The applicable rate of brokerage shall be clearly mentioned on the client registration form. The rate of brokerage as mentioned on the client registration form may further be revised upwards or downwards, by:

a. The client on giving a request to this effect, subject to approval by Agroy
b. Agroy at its discretion on giving a 15 days notice to the client
c. Agroy to comply with any directive of the stock exchange / SEBI or Government

Rate of brokerage shall not exceed the following upper limits prescribed by law for the time being:

a. For Cash Market Segment: The maximum brokerage chargeable in relation to trades effected in the securities admitted to dealings on the Capital Market segment of the Exchange shall be 2.5 % of the contract price exclusive of statutory levies. It is hereby further clarified that where the sale / purchase value of a share is Rs.10/- or less, a maximum brokerage of 25 paise per share may be collected.

b. For Option contracts: Brokerage for option contracts shall be charged on the premium amount at which the option contract was bought or sold and not on the strike price of the option contract. It is hereby clarified that brokerage charged on options contracts shall not exceed 2.5% of the premium amount or Rs 100/- (per lot) whichever is higher.

2. Imposition of various taxes / levies

The client shall pay all taxes, duties, levies imposed by any authority including but not limited to the stock exchanges (including any amount due on account of reassessment / backlogs etc.), transaction expenses, incidental expenses such as postage, courier etc. as they apply from time to time to the client's account / transactions / services that the client avails from Agroy.

The following taxes / levies for the time being in force shall be charged to the clients over and above the applicable rate of brokerage:

i. Securities Transaction Tax (STT)
ii. Stamp Duty
iii. Service Tax
iv. Exchange Transaction / Turnover Charges / Tax

3. Other Charges

Other transaction / service and incidental charges to be charged from clients include:

i. F&O Clearing Charges
ii. Postage / Courier Charges for issue of physical contract notes if specifically requested by the client
iii. Software / IBT Charges in case of Internet Based Trading Clients who have opted for Investor Trading Terminals.
iv. Any penalties / fines imposed or levied by Stock Exchange / SEBI on the positions of the client

4. Imposition of Penalty / delayed payment charges

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Agroy shall have the discretion to charge delayed payment charges to the client for delay in margin / payin obligation of the client at any time. The rate of such delayed payment charges shall be communicated to the client from time to time.

Agroy is entitled to impose fines / penalties for any orders / trades / deals / actions of the client which are contrary to the agreement / rules / regulations / bye laws of the exchange or any other law for the time being in force, at such rates and in such form as it may deem fit. Further where Agroy has to pay any fine or bear any punishment from any authority in connection with / as a consequence of / in relation to any of the orders / trades / deals / actions of the client, the same shall be borne by the client.

5. Payin of Funds & Securities

Agroy shall maintain centralized banking and securities handling processes and related banking and depository accounts at designated place for deposit of pay in from clients. The client shall ensure timely availability of funds/securities in designated form and manner at designated time and in designated bank and depository account(s) at designated place, for meeting his/her/its pay in obligation of funds and securities.

The details of all designated collection bank accounts shall be communicated by Agroy to the client. The client shall be responsible to make the payment of margins / obligations in the designated bank accounts only, and intimate Agroy of such deposit.

In case the payment of the margin / obligation is made by the client through a bank instrument, Agroy shall give the benefit / credit for the same only on the realization of the funds from the said bank instrument etc.

Payments made by the client from his own bank account or demat account shall only be accepted by Agroy. Agroy shall have an adequate systems and procedures in place to check third party transfers received from the client if any.

Payments from any client shall not be accepted in cash.

Detailed Procedure for Payin of Funds / Banking is explained in Appendix D

6. Payout of Funds & Securities

Agroy shall maintain centralized banking and securities handling processes and related banking and depository accounts at designated place for payout to clients.

All payout requests received from the clients shall be processed by Agroy within 24 hours of receiving such request.

Agroy has a right to make the payout from any of the designated bank accounts by way of any cheque / DD / wire transfer / RTGS / NEFT / etc. any other mode of banking transactions at the discretion of Agroy.

7. Running Account Authorisation & Maintenance

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

As per the SEBI / stock exchange guidelines, Agroy shall obtain running account authorisation from the clients. As per the running account authorisation, Agroy shall keep debiting or crediting the account of the client with daily obligations and/or margins. The balance to the credit of the client may be retained by Agroy until payout is requested by the client.

Notwithstanding the running account authorisation, the funds and security account of all clients must be settled by Agroy atleast once in every calendar month / calendar quarter as specifically opted by the client.

Agroy shall put in place an adequate system and procedure for such periodic settlement of client accounts keeping in mind the following guidelines:

i. Every client account shall be settled on any day during the period of calendar quarter or month as specified by the client.
ii. Adequate funds/securities can be retained by Agroy to meet the pending obligation of clients across various exchanges / segments, foreseen margin requirement based on current outstanding position of the client, unbilled charges if any, etc. subject to approved guidelines of the stock exchanges / SEBI
iii. Accounts which have a debit balance on any day during the given period shall be deemed to have been settled during the period.
iv. Accounts with a credit balance of less than Rs.500/- shall be deemed to be settled.
v. A settlement letter with account statements shall be sent by email to the client within 7 days of such settlement of account.

Agroy shall not be entitled to pay any interest to any client on credit balances of the client. The margin / security deposited by the client with Agroy are not eligible for any interest.

Agroy is entitled to include / appropriate any / all payout of funds & / or securities towards margin / security without requiring specific authorizations for each payout. Agroy is entitled to transfer funds &/ or securities from his account for one exchange & / or one segment of the exchange to his / her / its account for another exchange & / or another segment of the same exchange whenever applicable and found necessary by Agroy. Agroy is authorised by the client to treat / adjust his/ her / its margin / security lying in one exchange & / or one segment of the exchange / towards the margin / security / pay in requirements of another exchange & / or another segment of the exchange.

The clients shall have a discretion to withdraw the running account authorisation by giving a written notice to the Company at any time.

8. Shortages in obligations arising out of internal netting of trades

Stock broker shall not be obliged to deliver any securities or pay any money to the client unless and until the same has been received by Agroy from the exchange, the clearing corporation/ clearing house or other company or entity liable to make the payment and the client has fulfilled his / her/ its obligations first. The policy and procedure for settlement of shortages in obligations arising out of internal netting of trades is as under:

a. The securities delivered short are purchased from market on T+3 day which is the Auction Day on Exchange, and the purchase consideration (inclusive of all statutory taxes & levies) is debited to the short delivering seller client.
b. If securities cannot be purchased from market due to any reason whatsoever on T+3 day they can be covered from the market on any subsequent trading days. In case

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

any reason whatsoever (any error or omission) any delay in covering of securities leads to higher losses, stock broker will not be liable for the same. Where the delivery is matched partially or fully at the Exchange Clearing, the delivery and debits/credits shall be as per Exchange Debits and Credits.

c. In cases of securities having corporate actions all cases of short delivery of cum transactions which cannot be auctioned on cum basis or where the cum basis auction payout is after the book closure / record date, would be compulsory closed out at higher of 10% above the official closing price on the auction day or the highest traded price from first trading day of the settlement till the auction day.

9. Communication & Reports sent to Clients

- A Welcome Letter with account operating guidelines, client master sheet, copy of client registration form and delivery instruction booklet is sent to the client within 7 days of opening of the account.
- A welcome email is sent to all the clients within 7 days of opening of the account.
- A welcome-cum-verification telephone call is given to all the clients from Agroy Head Office at time of opening of client account.
- Agroy sends a statement of funds and securities to all the clients on a monthly basis by email.
- Agroy sends a printed statement of funds and securities for all the clients on a quarterly basis to the registered address of the client by post.
- Agroy also sends a statement of funds and securities to all clients within 7 days of the quarterly settlement of their account by email.
- Digitally signed contract notes are sent to all the clients within 24 hours of the trade by email. These contract notes are also available for download from our web-based accounts interface.
- Trade confirmations are sent to all the clients by SMS within 24 hours of the trade.
- Financial Balance SMS is sent to all clients on weekly basis.
- Margin Statements are sent to the clients alongwith their statements of Accounts on monthly basis.
- A Web based accounts interface is available for all the clients to login and view or print their account statements and various accounts related reports.
- A feedback call is made or feedback questionnaire is sent to random clients on a monthly basis to ascertain customer feedback on service standards.

IMPORTANT NOTE
We do not accept cash from clients under any circumstances
We do not offer portfolio management services and do not guarantee any returns on investment to clients

All clients, employees and associates of AGROY agree to have read and understood this master policy document and agree to abide by it at all times.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix A:
PREVENTION OF MONEY LAUNDERING (PMLA) POLICY

This policy is applicable for all segments including Cash, Equity Derivatives, Currency Derivatives and Depository Services related to Agroy Finance and Investment Limited and Commodity Derivatives related to Agroy Commodities Private Limited

1. INTRODUCTION

1. Money Laundering may be defined as cleansing of dirty money obtained from legitimate or illegitimate activities including drug trafficking, terrorism, organized crime, fraud and many other crimes with the objective of hiding its source and rendering it in legally usable form. It is any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. The process of money laundering involves creating a web of financial transactions so as to hide the origin of and true nature of these funds.
2. Successful money laundering activity spawning yet more crime exists at a scale that can and does have a distorting and disruptive effect on economies, marketplaces, the integrity of jurisdictions, market forces, democracies etc. It is in short a cancer, existing for one purpose only, to make crime and illegal activity worthwhile.
3. The general assembly of United States adopted the political declaration and global program of action in 1990 in its worldwide drive against money laundering and also enjoined upon member states to adopt legislation and program against laundering on a national level. India enacted the Prevention of Money Laundering Act, 2002. (Hereinafter referred to as 'Act'). The Prevention of Money Laundering Act, 2002 has come into effect from 1st July, 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July, 2005 by the Department of Revenue, Ministry of Finance, and Government of India.
4. Securities and Exchange Board of India (hereinafter referred to as SEBI) vide its Circular Ref No.: ISD/CIR/RR/AML/1/06 dated January 18, 2006 laid down broad guidelines on Anti Money Laundering Standards. As per the Circular, all the intermediaries registered with SEBI under Section 12 of the SEBI Act were advised to ensure that a proper policy framework on anti-money laundering measures was put in place. This was essentially in conformity with the Prevention of Money Laundering Act, 2002 and the Rules framed there under by SEBI.
5. AGROY Finance and Investment Ltd being such intermediary had in accordance with the above, in a Board Meeting Held on 3rd December, 2007 adopted a policy framework on anti-money laundering measures. Further, AGROY Commodities Pvt Ltd being such intermediary had in accordance with the above, in a Board Meeting Held on 1st December, 2009 adopted a policy framework on anti-money laundering measures.
6. In the light of Circulars issued by National Stock Exchange of India Ltd (hereinafter referred to as "NSE") and Circulars issued by Bombay Stock Exchange Ltd. (hereinafter referred to as "BSE"), in continuation to the new circular of Securities and Exchange Board of India (hereinafter referred to as "SEBI") SEBI Circular No. ISD/AML/CIR-1/2009 dated September 01, 2009 has issued additional requirements to be fulfilled and clarifications with regard to existing requirements mentioned in the Master Circular on Anti Money Laundering (AML) issued vide SEBI circular no. ISD/AML/CIR-1/2008 dated December 19, 2008.
7. *Money Laundering in India*: With the growing financial sector, India is vulnerable to money laundering activities. Some common sources of illegal proceeds in India are narcotics trafficking, illegal trade in gems, smuggling, corruption and income tax evasion. Large portions of illegal proceeds are laundered through the alternative remittance system called "hawala". Under this system, individuals transfer funds from once country to another or from one state to another, often without the actual movement of currency
8. *Prevention of Money Laundering Act, 2002*: To combat money-laundering activities, the Government of India enacted the Prevention of Money Laundering Act, 2002 (hereinafter referred to as the "Act") on January 17, 2003.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

The basic objective of the Act is three fold, viz.:

- To prevent, combat and control money laundering.
- To confiscate and seize the property obtained from the laundered money.
- To deal with any other issue connected with money laundering in India.

2. OUR PREVENTION OF MONEY LAUNDERING POLICY .

1. The purpose of this policy is to set out the prevention of money laundering commitments and obligations for AGROY Finance and Investment Ltd and AGROY Commodities Pvt Ltd (hereinafter collectively referred to as 'Company')
2. This policy is based on the provision of the "Prevention of Money Laundering Act, 2002 and circular issued by SEBI/FMC and exchanges thereof".
3. This internal policy sets out and establishes governing principles, broad guidelines and standards to be adopted by the Companies in order to protect the Companies from being used by any person to launder money.
4. Policy objectives
   - To protect *the Company from* being used for money laundering
   - To follow thorough "Know Your Customer" (KYC) policies and procedures in the day-to-day business.
   - To take appropriate action, once suspicious activities is detected, and make report to designated authorities in accordance with applicable law / laid down procedures.
   - To comply with applicable laws as well as norms adopted internationally with reference to Money Laundering.

3. THE MONEY LAUNDERING PROCESS.

3.1) Money can be obtained illegally from various criminal activities like drug trafficking, terrorism, organized crime and fraud. As criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities and provide a legitimate cover for their source of income they usually follow three stages:

1. **Placement** - This is where the criminal proceeds are first-injected into the system. It is also the stage where those who are educated, briefed and alert to the process of money laundering, have the best chance of detecting what is happening and are thus best able to thwart and disrupt the process at the outset.

   At this stage, very often larger amounts of money are divided and distributed into smaller amounts to avoid suspicion and then paid into a series of bank accounts, arose to purchase securities, or life policies or other assets, sometimes many kinds of assets, all to achieve the prime purpose of being able to inject the tainted money or value into the legitimate mainstream financial/business system.
   Eg: A criminal having huge crime proceeds in form of cash, can deposit this cash in bank accounts maintained with difference banks, in the name of his relatives, friends and associates, in small amounts.

2. **Layering** - After the injection has taken place and the tainted money or value has entered and become mixed up in the main mass of money or value in the financial system, it is spun around different accounts, different names, different ownerships, plus different instruments and investments.

   All these movements are designed to disguise the origins of the money or value and thus confuse those who might be attempting to trace the money or value back to the root, criminal source.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Facilitated by the birth of electronic funds transfer technology the fast movement of funds through multiple jurisdictions often with different laws, creates major problems for investigators of identification, access and ultimately achieving successful prosecutions.

3. **Integration**- Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

   Integration means the reinvestment of those funds in an apparently legitimate business so that no suspicion of its origin remains and to give the appearance of legitimizing the proceeds

3.2) Section 3 of the Prevention of Money Laundering Act, 2002 defines the offences or laundering. In terms, of this section whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of an offence of money laundering.

3.3) The term proceeds of crime have been defined under Section 2(u)of the Act viz:

"Any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property."

The said section broadly states that if a person is involved in the process of projecting proceeds of crime as untainted property then he shall be guilty of money laundering, for indulging in the said process of the following three elements / activities shall play a very important role:

Possession or ownership of the proceeds of crime or property acquired from proceeds of crime, which is being reflected as untainted property.

Transactions relating to proceeds of crime like converting its form

3.4) Concealment of the original transaction and/or creating ghost transactions from concealing actual transactions.
E.g. Possessing Benami Property, Unexplained cash credits, unexplained expenditure, bogus or fictitious accounts, unexplained investments.

4. APPLICABILITY

4.1) The Prevention of Money Laundering Policy applies to AGROY Finance and Investment Ltd and AGROY Commodities Pvt. Ltd.

In terms of rules framed under the Act, inter aila, every intermediary shall

1. Maintain a record of all transactions, the nature and value of which may be prescribed, whether such transactions comprise of single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month;

2. Furnish information of transactions referred to in Clause (a) to the Director within such time as may be prescribed;

3. Verify and maintain the records of the identity of all its Clients, in such a manner as may be prescribed

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

As per provision of section 2(n) of the Act, term "Intermediary" means: "A stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992 (15 of 1992);

Further in terms of rules made under the Act, all intermediaries shall maintain a record of:

1. all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
2. all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;
3. all cash transaction where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
4. all suspicious transactions whether or not mage in cash;
5. identity and current address or addresses including permanent address or addresses of the Client, the nature of business of the Client and his financial status; Provided that where it is not possible to verify the identity of the Client at the time of opening an account or executing any transaction, the banking company, financial institution and intermediary, as the case may be, shall verify the identity of the Client within a reasonable time after the account has been opened or the transaction has been executed.

Under these circumstances the Act, applies to AGROY Finance and Investment Ltd., and AGROY Commodities Pvt Ltd.

4.2) Suspicious Transactions

Suspicious transactions involve funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under the law; The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction

4.3) Criteria in relation to defining

It is difficult to define exactly what constitutes suspicious transactions and as such given below is a list of circumstances where transactions may be considered to be suspicious in nature. This list is only inclusive and not exhaustive. Whether a particular transaction is actually suspicious or not will depend on the background, details of the transactions and other facts and circumstances.

1. Complex /unusually large transactions/ patterns which appear to have no economic purpose.
2. Client having suspicious background or links with known criminals
3. Clients whose identity verification seems difficult.

For Example:

i. False identification documents
ii. Identification documents which could not be verified within reasonable time
iii. Non face to face Client

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

iv. Doubt over the real beneficiary of the account
v. Accounts opened with names very close to other established business entities.

4. Client appears not to co-operate.
5. Use of different accounts by Client alternatively.
6. Sudden activity in dormant accounts
7. Multiple accounts
   i. Large number of account having a common account holder, authorized signatory with no rationale
   ii. Unexplained transfers between multiple accounts with no rationale
8. Asset management services for clients where the sources of funds is not clear or not in keeping with the clients' apparent standing/business activity
9. Substantial increase in business without apparent cause (Unusual activity compared to past transactions)
10. Activity materially inconsistent with what would be expected from declared business
11. Inconsistency with clients apparent financial standing
12. Any account used for circular trading
13. Unusual transactions by Clients of Special Category (CSCs) and business undertaken by shell corporations, offshore banks/financial services, businesses reported to be in the nature of export-import of small items
14. A transaction which gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime.
15. A transaction which appears to be a case of insider trading
16. Transactions reflect likely market manipulations
17. Suspicious off market transactions
18. Value of transaction just under the reporting threshold amount in an apparent attempt to avoid reporting
19. Inconsistency in the payment pattern by the client
20. Trading activity in account of high risk clients based on their profile, business pattern and industry segment
21. Accounts based as 'passed through'. Where no transfer of ownership of securities or trading is occurred in the account and the account is being used only for funds transfers / layering purposes.
22. Large deals at prices away from the market
23. Suspicious off market transactions
24. Purchases made in one client's account and later on transferred to a third party through off market transactions through DP Accounts;
25. Multiple transactions of value just below the threshold limit specified in PMLA so as to avoid possible reporting;

4.4) Implementation of the above requirements for our activities

1. Company Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

2. Principal Officer Designation and Duties

The company has designated Shri. Ashish Kumar Gupta as the Principal Officer for its Anti-Money Laundering Program, with full responsibility for the company's AML program is qualified by experience, knowledge and training. The duties of the Principal Officer will include monitoring the company's compliance with AML obligations and overseeing communication and training for employees. The Principal

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Officer will also ensure that proper AML records are kept. When warranted, the Principal Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU – IND)

The company has provided the FIU with contact information for the Principal Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. The company will promptly notify FIU of any change to this information.

3. Designated Director and Duties

Agroy Finance and Investment Ltd has designated Shri. Tushar Agarwal as the Designated Director and Agroy Commodities Pvt Ltd has designated Smt Priya Agarwal as the Designated Director for its Anti-Money Laundering Program, to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules.

4. Customer Acceptance, Identification and Verification

At the time of opening an account or executing any transaction with it, the company will verify and maintain the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status as under

Constitution of Client	**Proof of Identity**	**Proof of Address**	**Others**
Individual	• PAN Card	• Copy of Bank Statement, etc	• N.A.
Company	• PAN Card • Certificate of incorporation • Memorandum and Articles of Association • Resolution of Board of Directors	• As above	• Proof of Identity of the Directors/Others authorized to trade on behalf of the company
Partnership Firm	• PAN Card • Registration certificate • Partnership deed	• As above	• Proof of Identity of the Partners/Others authorized to trade on behalf of the firm
Trust	• PAN Card • Registration certificate • Trust deed	• As above	• Proof of Identity of the Trustees/ others authorized to trade on behalf of the trust
AOP/ BOI	• PAN Card • Resolution of the managing body • Documents to collectively establish the legal existence of such an AOP/ BOI	• As above	• Proof of Identity of the Persons authorized to trade on behalf of the AOP/ BOI

1. If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our company will not open the new account.
2. All PAN Cards received will verified form the Income Tax/ NSDL website before the account is opened
3. The company will maintain records of all identification information for eight years after the account has been closed

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

5. Reliance on Third Party for carrying out Due Diligence

We may rely on a third party for the purpose of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. Further, we shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

6. Verification against List of Designated Individuals/Entities

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at **http://www.un.org/sc/committees/1267/consolist.shtml**. We shall ensure that accounts are not opened in the name of anyone whose name appears in said list.

Further, we shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIU-IND.

7. Risk-based Approach

It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction etc. As such, Agroy should apply each of the customer due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that Agroy shall adopt an enhanced customer due diligence process for higher risk categories of customers. Conversely, a simplified customer due diligence process may be adopted for lower risk categories of customers.

All the clients of Agroy should be categorised into High, Medium and Low Risk categories. A system should be put in place to generate alerts based on trading pattern and dealing of clients which would enable to review the classification of clients from time to time.

In line with the risk-based approach, the type and amount of identification information and documents that registered intermediaries should obtain necessarily depend on the risk category of a particular customer.

8. Clients of special category (CSC):

Such clients include the following:
a. Non resident clients
b. High networth clients,
c. Trust, Charities, NGOs and organizations receiving donations
d. Companies having close family shareholdings or beneficial ownership
e. Politically exposed persons (PEP) of foreign origin
f. Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
g. Companies offering foreign exchange offerings
h. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens /

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.
i. Non face to face clients
j. Clients with dubious reputation as per public information available etc.
The above mentioned list is only illustrative and AGROY should exercise independent judgment to ascertain whether new clients should be classified as CSC or not.

9. Maintenance of records

The Principal Officer will be responsible for the maintenance for following records

- all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;
- all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- all suspicious transactions whether or not made in cash. Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith -
  - gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
  - appears to be made in circumstances of unusual or unjustified complexity; or
  - appears to have no economic rationale or bonafide purpose; or
  - gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

The records shall contain the following information:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction."

The records will be updated on daily basis, and in any case not later than 5 working days

10. Monitoring Accounts For Suspicious Activity

The company will monitor through the automated means of Back Office Software for unusual size, volume, pattern or type of transactions. For non automated monitoring, the following kinds of activities are to be mentioned as Red Flags and reported to the Principal Officer.

- The customer exhibits unusual concern about the company's compliance with government reporting requirements and the company's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the company's policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the Rs.10,00,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer insists for multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the company's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as Z group and T group stocks, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

When a member of the company detects any red flag he or she will escalate the same to the Principal Officer for further investigation

Broad categories of reason for suspicion and examples of suspicious transactions for an intermediary are indicated as under:

Identity of Client
- False identification documents
- Identification documents which could not be verified within reasonable time
- Non-face to face client
- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities

Suspicious Background
- Suspicious background or links with known criminals

Multiple Accounts
- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- Unexplained transfers between multiple accounts with no rationale

Activity in Accounts
- Unusual activity compared to past transactions
- Use of different accounts by client alternatively
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business
- Account used for circular trading

Nature of Transactions
- Unusual or unjustified complexity
- No economic rationale or bonafide purpose
- Source of funds are doubtful
- Appears to be case of insider trading
- Investment proceeds transferred to a third party
- Transactions reflect likely market manipulations
- Suspicious off market transactions

Value of Transactions
- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Large sums being transferred from overseas for making payments
- Inconsistent with the clients apparent financial standing

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

- Inconsistency in the payment pattern by client
- Block deal which is not at market price or prices appear to be artificially inflated/deflated

11. Reporting to FIU IND

For Cash Transaction Reporting

- All dealing in Cash that requiring reporting to the FIU IND will be done in the CTR format and in the matter and at intervals as prescribed by the FIU IND

For Suspicious Transactions Reporting

We will make a note of Suspicion Transaction that have not been explained to the satisfaction of the Principal Officer and thereafter report the same to the FIU IND and the required deadlines. This will typically be in cases where we know, suspect, or have reason to suspect:

- the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any the transaction reporting requirement,
- the transaction is designed, whether through structuring or otherwise, to evade the any requirements of PMLA Act and Rules framed thereof
- the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or
- the transaction involves the use of the company to facilitate criminal activity.

We will not base our decision on whether to file a STR solely on whether the transaction falls above a set threshold. We will file a STR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities.

All STRs will be reported quarterly to the Board of Directors, with a clear reminder of the need to maintain the confidentiality of the STRs.

We shall maintain and preserve the record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, for a period of eight years from the date of the transaction.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the PMLA Act and Rules thereof.

12. Screening of Employees while hiring

While hiring the employees, valid Copy of PAN Card, Address proof other ID card is obtained from the previous employer and their names are verified from the site of AMNI and CPAI as to whether they are not debarred from accessing the stock/commodity market.

Proper training is being provided to all the employees from time to time to make them conversant with the latest developments of the security/Commodity market.

13. Procedure for freezing funds, financial assets or economic resources or related services

Section 51A, of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated August 27, 2009 detailing the procedure for the implementation of Section 51A of the UAPA. Under the aforementioned Section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

We shall ensure the effective and expeditious implementation of said Order by following the steps laid out vide SEBI Circular ref. no: ISD/AML/CIR-2/2009 dated October 23, 2009, which needs to be complied with scrupulously.

14. AML Record Keeping

a. STR Maintenance and Confidentiality
We will hold STRs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a STR. We will refuse any requests for STR information and immediately tell FIU IND of any such request we receive. We will segregate STR filings and copies of supporting documentation from other company books and records to avoid disclosing STR filings. Our Principal Officer will handle all requests or other requests for STRs.

b. Responsibility for AML Records and SAR Filing
Principal Officer will be responsible to ensure that AML records are maintained properly and that STRs are filed as required

c. Records Required
As part of our AML program, our company will create and maintain STRs and CTRs and relevant documentation on customer identity and verification. We will maintain STRs and their accompanying documentation for at least eight years.

15. Investor Awareness

We will guide and inform all clients about the provisions of PMLA at the time of opening the account with us. Further, investors shall be educated about the provisions of PMLA by way of our website and mailers.

16. Program to Test AML Program

a. Staffing
The testing of our AML program will be performed by the Statutory Auditors of the company

b. Evaluation and Reporting
After we have completed the testing, the Auditor staff will report its findings to the Board of Directors. We will address each of the resulting recommendations.

17. Hiring of Employees

We shall carry out due diligence of new employees at the time of hiring them. This will include obtaining and verifying the Photo Identity and Address Proof. Also verification of the credentials of all new employees shall be done through reference check with past employers and other references as may be applicable.

18. Training Programs

We will develop ongoing employee training under the leadership of the Principal Officer. Our training will occur on at least an annual basis. It will be based on our company's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the company's compliance efforts and how to perform them; the company's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PMLA Act.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

We will develop training in our company, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

19. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer. We will also review the AML performance of supervisors, as part of their annual performance review. The Principal Officer's accounts will be reviewed by the Board of Directors

20. Periodic Review of this AML Policy

The company shall undertake periodic review of this policy to update it in accordance with the PMLA and various circulars issued by SEBI and Exchanges. Such review may carried out as and when deemed fit but atleast once in every financial year.

21. Confidential Reporting of AML Non-Compliance

Employees will report any violations of the company's AML compliance program to the Principal Officer, unless the violations implicate the Principal/Compliance Officer, in which case the employee shall report to the Chairman of the Board, Mr./Ms. Such reports will be confidential, and the employee will suffer no retaliation for making them.

22. Board of Directors Approval

We have approved this AML program as reasonably designed to achieve and monitor our company's ongoing compliance with the requirements of the PMLA and the implementing regulations under it.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix B:
PROHIBITION OF INSIDER TRADING POLICY

SEBI has enacted the Prohibition of Insider Trading Regulations, 2002 AND subsequent insider trading regulations 2009, which is applicable to all market intermediaries like Agroy Finance and Investment Ltd. Pursuant to the said regulations and amendments in the said regulations from time to time, it is necessary that Agroy Finance and Investment Ltd being a capital market intermediary, do comply and follow the prescribed procedures in order to prevent the misuse of price sensitive information which an employee/client/director/officer of the company may have access to.

The Board of Directors at their meeting held on 05/11/2012 have examined the provisions of the said Regulations and have amended the code of trading in securities by all the Employee/clients.

For the purposes of implementation of the code for trading in securities by employee/clients, definitions along with explanations where thought necessary are given as under:

I. DEFINITIONS:

"**Securities**" include-
(i) Shares, scrips, stocks, bonds, debentures, debenture stock or other marketable securities of a like nature in or of any incorporated company or other body corporate;
(ii) Derivative;
(iii) Units or any other instrument issued by any collective investment scheme to the investors in such schemes;
(iv) Government securities;
(v) Such other instruments as may be declared by the Central Government to be securities; and
(vi) Rights or interests in securities.
Explanation: Mutual fund units, derivative products like futures and options are also covered.

"**Client Company**" means a listed company which has given mandate or proposes to give any mandate in relation to preparation of any research report, credit rating report, appraisal report or valuation report. "Compliance Officer" means a senior officer(s) of the Company who are appointed as Compliance Officer(s) for overseeing the compliance with Prohibition of Insider trading.

"**Price Sensitive Information**" means any information which relates directly or indirectly to a company and which if published is likely to materially affect the price of securities of such company and includes-
- periodical financial results of the Company
- intended declaration of interim/final dividend
- issue of securities or buy-back of securities
- any expansion plans or execution of new projects
- amalgamation, mergers or takeovers,

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

• disposal of the whole or substantially the whole of the undertaking, any significant changes in policies, plans or operations of the Company

II. Basic procedures for personal investments:

Moral conduct: Every employee/client is expected to put the interest of the Company before his/her personal interest.

Prevention of misuse of Price Sensitive Information: Employee/clients should not use price sensitive information to buy or sell securities of any sort, whether for their own account or relatives.

Transactions: All Employee/clients should do all their transactions only through Agroy Finance and Investment Ltd.

No Speculation or short sales permitted: Employee should not speculate in shares/derivatives. All purchase transactions have to be delivery based. Selling securities for which delivery has not been taken is prohibited.

Front Running transactions are strictly prohibited. Front running means transacting in a security knowing fully well that Agroy Finance and Investment Ltd also intends to transact in the same security if any.

No passing of price sensitive information: Designated Employee/clients/Directors/ Dependent Persons are prohibited from passing on information to anybody inducing him/her to buy/sell securities.

Special Restrictions of Employee / Clients in research department:
Designated Employee/clients/Directors working as Research Analysts for preparing research reports of a client company shall disclose their shareholding/interest in such company to the compliance officer and shall not trade in securities of such client company for a period of atleast 30 days from publication /preparation of such report. For this purpose, any employee/client in the research department should inform the company's name of which is preparing a report and give an undertaking in the format prescribed in Annexure In case any employee/client leaves Agroy Finance and Investment Ltd, he/she shall be required to give an undertaking that he/she will not deal with any transaction on the basis of unpublished price sensitive information.

Penalty for contravention of code of conduct
Any Directors/Designated employee/clients/dependent persons who trades in securities or communicates any information or counsels any person trading in securities, in contravention of this code of conduct may be penalised and appropriate action may be taken against him, which may include disciplinary action by the company, which may include wage freeze, suspension, etc.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix C:
RISK MANAGEMENT & SURVEILLANCE POLICY

INTRODUCTION:

National Stock Exchange of India Limited (NSE) vide its circular dated 7th March 2013 has directed the trading members to frame the surveillance policy for effective monitoring of Trading Members and monitoring the alerts based on trading activity on the Exchange. Trading members are directed to have proper mechanisms and to ensure that proper checks and balances are in place.

POLICY:

The Company shall implement the following policy:-

1) Transactional Alerts to be provided by the exchange:

In order to facilitate effective surveillance mechanisms, the Firm would download the below mentioned alerts based on the trading activities on the exchanges.

Sr. No.	Transactional Alerts	Segment
1	Significantly increase in client activity	Cash
2	Sudden trading activity in dormant account	Cash
3	Clients/Group of Client(s), deal in common scrips	Cash
4	Client(s)/Group of Client(s) is concentrated in a few illiquid scrips	Cash
5	Client(s)/Group of Client(s) dealing in scrip in minimum lot size	Cash
6	Client / Group of Client(s) Concentration in a scrip	Cash
7	Circular Trading	Cash
8	Pump and Dump	Cash
9	Wash Sales	Cash
10	Reversal of Trades	Cash
11	Front Running	Cash
12	High Turnover Concentration	Cash
13	Order Book Spoofing i.e. large orders away from market	Cash

The Firm may formulate its own alerts in addition to above mentioned type of alerts.

2) Clients Information:

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

The Company will carry out the Due Diligence of its client(s) on a yearly basis. Further, the Company shall ensure that key KYC parameters are updated on a yearly basis and latest information of the client is updated in Unique Client Code (UCC) database of the Exchange. Based on this information the Company shall establish groups / association amongst clients to identify multiple accounts / common account / group of clients.

3) Analysis:

In order to analyze the trading activity of the Client(s) / Group of Client(s) or scrips identified based on above alerts, the Company will carry out the following procedure:

a. To seek explanation from such identified Client(s) / Group of Client(s) for entering into such transactions.
b. To Seek documentary evidence such as bank statement / demat transaction statement or any other documents as below:
    a. In case of funds, Bank statements of the Client(s) / Group of Client(s) from which funds pay-in have been met, to be sought. In case of securities, demat account statements of the Client(s) / Group of Client(s) from which securities pay-in has been met, to be sought.
    b. The period for such statements may be at least 15 days from the date of transactions to verify whether the funds / securities for the settlement of such trades actually belongs to the client for whom the trades were transacted.
c. The Company shall review the alerts based upon:
    a. Type of the alerts downloaded by the exchange
    b. Financial details of the clients
    c. Past Trading pattern of the clients/ client group
    d. Bank /Demat transaction details
    e. Other connected clients in UCC (common email/mobile number/address, other linkages, etc)
    f. Other publicly available information.
d. After analyzing the documentary evidences, including the bank / demat statement, the Firm will record its observations for such identified transactions or Client(s) / Group of Client(s). In case adverse observations are recorded, the Compliance Officer shall report all such instances to the Exchange within 45 days of the alert generation. The Firm may seek extension of the time period from the Exchange, wherever required.

4) Monitoring and reporting:

For effective monitoring, the Company;

1. Within 30 days of alert generation shall dispose off the alert, and any delay in disposition, reason for the same shall be documented.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

2. In case of any Suspicious or any Manipulative activity is identified, the same will be mentioned in the Register to be maintained for the purpose and will be reported to the Stock Exchanges within 45 days of the alert generation.
    a. The Company shall prepare quarterly MIS and shall put to the Directors on the number of alerts pending at the beginning of the quarter, generated during the quarter, disposed off during the quarter and pending at the end of the quarter. Reasons for pendency shall be discussed and appropriate action shall be taken. Also, the Board shall be apprised of any exception noticed during the disposition of alerts. The surveillance process shall be conducted under overall supervision of its Compliance Officer. Compliance Officer would be responsible for all surveillance activities carried out by the Company and for the record maintenance and reporting of such activities.
    b. Internal auditor of the Company shall review the surveillance policy, its implementation, effectiveness and review the alerts generated during the period of audit. Internal auditor shall record the observations with respect to the same in their report.

5) Policy on Facility of Voluntary Freezing / Blocking the online access to the trading account to clients on account of suspicious activities:

(per requirements of SEBI Circular No. SEBI/HO/MIRSD/POD-1/P/CIR/2024/4 dated January 12, 2024)

1. The clients may request for voluntary freezing/ blocking the online access of trading account if any suspicious activity is observed in the trading account vide either of the following channels:
    a. Send an email from their registered email id to stoptrade@agroy.com
    b. Send SMS from their registered Mobile No to 8448897103
    c. Send Whatsapp from their registered Mobile No to 8448897100
    d. Give a call on 8448897101

2. The company shall take the following actions on the receipt of request through any modes of communications as provided by the Trading Member for freezing/blocking of the online access of the trading account from the client:

    a. Validate that the request is received from the client and issue the acknowledgement as well as freeze/block the online access of the client's trading account and simultaneously cancel all the pending orders of the said client. The timelines for freezing/ blocking of the online access of the clients' trading account is as under: -

Scenario	Timelines for issuing acknowledgement as well as freezing / blocking of the online access of the trading account.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Request received during the trading hours1 and within 15 minutes before the start of trading.	Within 15 minutes
Request received after the trading hours and 15 minutes before the start of trading.	Before the start of next trading session

b. Post freezing/blocking the client's trading account, the Company shall send a communication on the registered mobile number and registered e-mail ID of the client, stating that the online access to the trading account has been frozen/blocked and all the pending orders in the client's trading account, if any, have been cancelled along with the process of re-enablement for getting the online access to the trading account.

c. Details of open positions (if any) shall be communicated to the client alongwith contract expiry information within one hour from the freezing/blocking of the trading account. This will eliminate the risk of unwanted delivery settlement. This time limit shall be contracted after a review in the next six months after the date of its applicability to enhance protection of investors from suspicious activities.

3. The Company shall have a mechanism in place to validate that the request for freezing/blocking of the online access of the trading account is received from the respective client only. This can be done by the Trading Member by:
   a. verifying whether request is received from the registered phone number/e-mail Id of the client; or where request is received from other than registered phone number/e-mail Id of the client, the Trading Member should have a client authentication procedure (2 Factor Authentication) in place or
   b. Following any other process as may be prescribed by the Exchange(s) uniformly in consultation with SEBI, from time to time.

4. The Company shall maintain the appropriate records/logs including, but not limited to, request received to freeze/block the online access of trading account, confirmation given for freezing/blocking of the online access of the trading account and cancellation of pending orders, if any, sent to the clients.

5. In case of failure of the Company in freezing/ blocking the online access within the prescribed timelines, the Company shall be responsible for any trades executed from the time of receipt of such request till such time the online access is blocked / frozen.

6. Re-enabling the client for online access of the trading account: - the Company shall re-enable the online access of trading account after carrying out necessary due diligence including validating the client request and unfreezing / unblocking the online access of the trading account.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix D:
PREFUNDED DOCUMENTS AND BANKING POLICY

SUMMARY OF BANK ACCOUNTS:

For Direct Cheque Deposit:

Bank Details	**For EQUITY / FO / CURRENCY / COMMODITIES**
Beneficiary Name	Agroy Finance and Investment Ltd
HDFC Bank	00030340000043
ICICI Bank	022505003532
Punjab National Bank	0117002101000911
State Bank of India	31188348544

For RTGS / NEFT:

Bank Details	**For EQUITY / FO / CURRENCY / COMMODITIES**
Beneficiary Name	Agroy Finance and Investment Ltd
A/c No	00030340000043
Location	New Delhi
Bank Name	HDFC Bank Ltd
Bank Branch	Asaf Ali Road, New Delhi
Type of A/c	Current
IFSC Code	HDFC0000003

Please send a payment intimation mail to banking@agroy.com clearly mentioning your account code and payment details.

DETAILED POLICY:

This Policy is to help you understand the process and guidelines for Payin and Payout of Funds.

Following are the main compliance issues to be observed with respect to banking:

1. The payment should be made by client from his own registered bank account. Payment should not be accepted from third party accounts.
2. Cash cannot be accepted under any circumstances.
3. DD/PO of upto Rs.50,000/- shall only be accepted. In case DD/PO is collected, a declaration in form attached as Form -1 should accompany the DD/PO.

Procedure for deposit of Cheque / DD / PO:

1. Clients can make payment to AGROY in 3 forms: (a) By Cheque; (b) By DD/PO (d) RTGS / NEFT
2. Cheques may be sent to AGROY HO directly after writing the client code on reverse of the Cheque or may be deposited locally by the Client / Franchisee in our designated Bank A/c.
3. DD / PO of more than Rs.50,000/- are not acceptable. DD / PO should always be payable at Delhi and sent to HO only. These should not be deposited locally directly by the client / franchisee. All DD / PO

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

must be accompanied by a **DD Declaration** in the specified format given below. In case the value of DD / PO exceeds Rs.50,000/- then it must accompany a certificate from the issuing bank verifying the name of the account holder and account number from which such DD / PO has been made. Following documents are acceptable in such cases:

a. Certificate from the issuing bank on its letterhead or on a plain paper with the seal of the issuing bank.
b. Certified copy of the requisition slip (portion which is retained by the bank) to issue the instrument.
c. Certified copy of the passbook/bank statement for the account debited to issue the instrument.
d. Authentication of the bank account-number debited and name of the account holder by the issuing bank on the reverse of the instrument.

4. For cheques deposited locally by the client / franchisee, following must be ensured:
   a. Entry of the cheque deposit must be made in the online back-office by you
   b. Photocopy of the cheque must be sent to HO by Fax / Email
   c. On receipt of the photocopy of cheque and on clearing of the cheque, the voucher entered by you in the backoffice is released by us and credit is given to the client.
5. In case of Online Fund Transfers / NEFT / RTGS, clients must ensure that such funds are transferred from their own designated bank account only. Funds received from Third Party Accounts shall not be accepted and returned.

Procedure for issue of Funds Payout:

1. All funds payout are done by way direct electronic fund transfer to the client's designated bank account by way of NEFT / RTGS.
2. For payout, please send us a request on e-mail at agroybanking@gmail.com. For all payout requests received by 3:00pm, the NEFT/RTGS instructions are issued to HDFC Bank on the same day. For email requests received after 3:00pm, the NEFT/RTGS instructions are issued to HDFC Bank on the next working day.
3. We do not have the facility of making payout by way of Demand Drafts / Pay Orders.

IMPORTANT: THIRD PARTY CHEQUES OR FUNDS DEPOSITED IN OUR ACCOUNT SHALL BE AT RISK OF THE CLIENT, SINCE NO CREDIT IS GIVEN FOR THE SAME. SUCH FUNDS ARE RETURNED TO BONAFIDE TRANSFEREE ACCOUNT ONLY.

FORMAT OF DD/PO DECLARATION

I / We hereby declare that Demand Draft No…….. dated ……. of Rs……

(Rupees ……) drawn on

……. Bank in favour of AGROY Finance & Investment Ltd / AGROY Commodities

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Pvt Ltd has been prepared by me/us from my/our own account. Copy of Demand Draft is enclosed herewith.

Date:……..

Client Sign: ……

Client Name: ……

Client Code: ……

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix E:
UNAUTHENTIC NEWS CIRCULATION POLICY

INTRODUCTION:

The purpose of this policy is to avoid the unauthenticated news circulation related to various scrips by employees without adequate caution. It has been observed that market news circulated through blogs/chat forums / email by employees without adequate caution can do considerable damage to the normal functioning and behavior of the market and distort the price discovery mechanisms.

POLICY:

The Company shall implement the following policy:-

- No staff member or associate is authorised to send any communication to any client by way of SMS / Email / Letter / Notice / etc., unless such communication is specifically authorised by the Compliance Officer / Designated Director
- Any Equity Research Reports, Advisory Notes and Stock Recommendations sent out to the client can be sent out only from a designated Sender ID and should be duly authorised by the Compliance Officer.
- Log of all such communication sent to the clients should be maintained.
- If any employee fails to follow these regulations he /she will be liable for strict actions

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix F:
INVESTOR GRIEVANCE REDRESSAL POLICY

The Company shall implement the following policy:-

- The designated Email ID for lodging investor complains is customercare@agroy.com
- The same has been clearly displayed on the website and on all information sent to the clients
- All the investor complaints received by email on the designated email ID should be duly saved and recorded in the investor grievances register.
- All investor grievances which are not redressed at the first level must be escalated to the next level within 7 days.

Investor Grievances Redressal System - Escalation Matrix:

First Level	Contact your dealer on phone or walk-in-to your dealing office and lodge the complaint in the complaint register of the dealing office.
Second Level	Send email to **customercare@agroy.com** Please quote your client code clearly in this email.
Third Level	Contact Centralized Helpdesk at AGROY Head Office Mr.Jitendra Singh Rawat on 8448897101 or at trade@agroy.com
Fourth Level	Contact central Compliance Officer at Head Office Mr.Ashish Kumar Gupta on 9312211869 or at ashish.gupta@agroy.com
Fifth Level	Contact Company Director Mr.Tushar Agarwal on 9810118281 or at Email:ceo@agroy.com
Sixth Level	Contact the Investor Grievance Cell of the concerned Exchange at: BSE – (011) 41510480 – iscdelhi@bseindia.com NSE – (022) 26598190 – ignse@nse.co.in CDSL – 18002005533 – complaints@cdslindia.com MCX – (022) 66494070 - grievance@mcxindia.com
Seventh Level	You can lodge your grievances with SEBI on http://scores.gov.in. For any queries, feedback or assistance, you may contact SEBI helpline on 1800227575 / 18002667575

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix G:
DOCUMENTED ERROR ACCOUNT POLICY

AGROY shall have the absolute discretion to accept, refuse or partially accept the client code Modification requests based on Risk Perception and other factors considered relevant by AGROY; AGROY and / or any of its directors, employees will not be held responsible for Damages/losses due to such refusal or due to delay caused by such review.

Client code modification requests will be strictly accepted only to rectify genuine error in entry of client code at the time of placing /modifying the related order; consequently dealers are expected to take utmost care/precaution while execution of client trades.

As per SEBI circular dated July 5, 2011 on client code modifications, penalty will be levied on all client code modifications w.e.f. August 1, 2011 (including genuine errors).

AGROY will allow Modifications in the client Codes of Non-Institutional clients only for the following objective Criteria provided there is no consistent pattern in such modifications:

- Error due to communication and / or punching or typing such that the original client code / name and the modified client code / name are similar to each other.

- Modification within relatives (Relative for this purpose would mean 'Relative' as defined under sec. 6 the Companies Act, 1956).

Any transfer of trade (institutional or non-institutional) to "ERROR ACCOUNT" of AGROY would not be treated as modification of client code and would not attract any amount of penalty, provided the trades in "ERROR ACCOUNT" are subsequently liquidated in the market and not shifted to some other client code. However operational costs as applicable & Profit / Loss from the transaction will be transferred to the concerned Dealer / Associate.

Client Code Modification requests through "ERROR ACCOUNT" will be accepted only till 3:30 PM IST.

All cases of modification of client codes of non-institutional trades executed on the Exchange, shall be liable for a penalty as laid down by regulators from time to time [As per SEBI Circular No. CIR/DNPD/6/2011 dated July 5, 2011 a penalty of 1% of value of non-institutional trades modified will be levied if value of non-institutional trades modified as a percentage of total value of non-institutional trades executed is less than or equal to 5% and penalty of 2% if modification exceeds 5%, in a segment during a month.

In addition to above it is well within rights of AGROY to levy additional penalties in case concerned Dealer/Associate fails to submit any sufficiently valid reason for client code Modification.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

AGROY will levy Penalties as applicable in relation to client code modification on next day of the Modification date, though Bills/Files in relation to same may be provided by exchange on a later date.

AGROY shall conduct a special inspection of the concerned Dealer/Associate, if modification exceeds 1% of the value of trades executed during a month and take appropriate disciplinary action, if any deficiency is observed.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix H:
LIMIT SETTING POLICY

In terms of Exchange requirements, Agroy has decided to implement the policy for setting up of trading limits on the exchange terminals.

The following policy shall be followed while setting up of limits:

1) Branch Buy/ Sell Limits
   a) In Equity Segment Branch Buy Value and Branch Sell value limits shall be set by the Corporate Manager.
   b) In F&O Segment and in CDS Segment Branch Buy Value and Branch Sell value limits shall be set by the Corporate Manager for both Futures and options.

2) Dealer Buy/ Sell Limits
   a) In Equity Segment Dealer wise Buy/ Sell Value limits shall be set by the Corporate Manager/ Branch Manager.
   b) In F&O Segment and in CDS Segment Buy/Sell Value Limits shall be set by Corporate Manager/ Branch Manager.

3) Order Value Limits Apart from setting up of branch/ terminal wise limits, Corporate Manager shall set Order value limits for both maximum order quantity and maximum order value.

4) Market Price protection Limit Corporate manager shall also set up market price protection limit for each dealer.

5) In equity segment Corporate manager may also set up symbol wise limit for each scrip as and when required.

6) Corporate manager shall review these limits from time to time and in case any amendment is made in existing limits, record of such modification shall be maintained.

7) Corporate manager shall ensure that none of the limits mentioned above has been set as Unlimited.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix I:
INACTIVE ACCOUNTS POLICY

INTRODUCTION:

There arises a need to temporarily suspend or permanently deregister certain client trading accounts in view of effective internal controls, protection of client account and to meet KYC compliances. Hence at Agroy we have framed a comprehensive policy on suspension and deregistration of client trading accounts.

POLICY:

The Company shall implement the following policy:-

Temporary Suspension of Inactive Client Trading Accounts:

Temporary Suspension of Client Trading Account are done by the Company at request of the client in following cases:

i. The client may request us to temporarily suspend his trading account by writing a letter or sending an email to the company.

Temporary Suspension of Client Trading Account are done by the Company at own discretion in following cases:

i. The address of the client becomes unverifiable due to the post / courier being sent to such address are repeatedly returned atleast three times.
ii. Continuous outstanding debit balance in client account for period of more than 90 days and the client not responding to various payin reminders of the company.
iii. Any alert / signal raised as per the PMLA policy of the company.
iv. Account remains dormant / inactive for a period of more than six months.
v. Annual renewal documents prescribed by the Exchange / SEBI are not submitted by the client.

The procedure adopted for temporarily suspending a client trading account is as follows:

i. A temporary suspension notice by way of email is sent to such a client clearly stating the reasons of suspension.
ii. In case of any outstanding position / debits in the client account, the company may initiate liquidation proceedings anytime after 7 days of sending the temporary suspension notice to the client.
iii. The funds and securities account are fully settled within 7 days of suspension of a client account.
iv. The account temporarily suspended can be reactivated after resolution of the reason of suspension and a request of reactivation received from the client.
v. In case temporary disablement is due to outstanding debit for more than 90 days, then a legal recovery notice may also be sent to the client.

De-registering a client account

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Notwithstanding anything to the contrary stated in the agreement, Agroy is entitled to terminate the agreement with immediate effect in any of the following circumstances:

i. If the actions of the Client are prima facie illegal/ improper or such as to manipulate the price of any securities or disturb the normal/ proper functioning of the market, either alone or in conjunction with others.
ii. If there is any commencement of a legal process against the Client under any law in force;
iii. On the death / lunacy or other disability of the Client;
iv. If a receiver, administrator or liquidator has been appointed or allowed to be appointed of all or any part of the undertaking of the Client;
v. If the Client has voluntarily or compulsorily become the subject of proceedings under any bankruptcy or insolvency law or being a company, goes into liquidation or has a receiver appointed in respect of its assets or refers itself to the Board for Industrial and Financial Reconstruction or under any other law providing protection as a relief undertaking;
vi. If the Client being a partnership firm, has any steps taken by the Client and/ or its partners for dissolution of the partnership;
vii. If the Client have taken or suffered to be taken any action for its reorganization, liquidation or dissolution;
viii. If the Client has made any material misrepresentation of facts, including (without limitation) in relation to the Security;
ix. If there is reasonable apprehension that the Client is unable to pay its debts or the Client has admitted its inability to pay its debts, as they become payable;
x. If the Client suffers any adverse material change in his / her / its financial position or defaults in any other agreement with Agroy;
xi. If the Client is in breach of any term, condition or covenant of this Agreement;
xii. If any covenant or warranty of the Client is incorrect or untrue in any material respect;
xiii. If the client account has remained in suspension for more than 1 year.
xiv. If an account closure request is received from the client.

The procedure adopted for closure of a client trading account is as follows:

i. A notice of closure by way of courier / registered post is sent to such a client clearly stating the reasons of closure.
ii. All such cases of closure are clearly recorded in an Account Closure Register.
iii. In case of any outstanding position / debits in the client account, the company may initiate liquidation proceedings anytime after 30 days of sending the closure notice to the client.
iv. The funds and securities account are fully settled within 7 days of closure of a client account.
v. Demat account closure proceedings are also initiated for the client simultaneously.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Appendix J:
CDSL SURVIELLENCE POLICY

INTRODUCTION:

This surveillance policy is defined based on the CDSL Circular No. CDSL/OPS/DP/SYSTM/2021/309 dated July 15, 2021. Surveillance is an integral part of any organization for monitoring the transactions based on the guidelines provided by the depository / SEBI from time to time.

Important Definitions:
1. Depository means CDSL
2. DP (Depository Participant) means Agroy Finance and Investment Ltd (AFIL)

POLICY:

A. Obligation of DP to frame the policy:

As per the above referred circular, every DP should frame the surveillance policy based on the business model adopted by the DP and the same approved by the Board. In this scenario, AFIL being the DP who is servicing the retail clients is required to generate the alerts to monitor the transactions executed in their depository system based on the following parameters and place this policy to obtain necessary approval from the Board:

a) Generation of suitable surveillance alerts based on the indicative themes which is given in point B.
b) Review and disposal of transactional alerts provided by depository (CDSL providing the transactional alerts once in 15 days to the DPs which required to be reviewed).
c) To generate own alerts apart from the above alerts provided by depository
d) Disposal of alerts within 30 days from the date of alerts generated at DP end and alerts provided by the Depository.
e) Reporting to Depository and other authorities as applicable, in case of any abnormal activity
f) Documentation of reasons for delay, if any, in disposition of alerts
g) Actions which required to be taken as per obligations under Prevention of Money Laundering (PMLA).
h) Record maintenance for the period as stipulated under applicable statutory authorities.
i) Review of surveillance policy once in a year by the DP.

B. Obligations of DP to generate additional surveillance alerts:

Based on the above guidelines, DP is required to generate the additional alerts apart from the alerts provided by Depository as per the themes provided below:

SN	Themes
1	Alerts for multiple demat accounts opened with the same demographic details. Alerts for accounts opened with same PAN / Mobile Number / Email IDs / Bank Account Number / Address considering the existing demat account held with DP
2	Alert for communication (email / letter) sent on registered email id / address of the clients are getting bounced
3	Frequent changes in details of demat account such as address, email id, mobile number, Authorised Signatory, PoA holder etc
4	Frequent off-market transfers by a client in a specified period
5	Off Market transfers not commensurate with the income / Networth of the client
6	Pledge transactions not commensurate with the income / Networth of the client

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

7	Off-Market transfers (High Value) immediately after modification of details in demat account
8	Review of reasons for Off-Market transfers provided by client for off-market transfers vis-à-vis profile of the client e.g. transfers with reason code Gifts with consideration, frequent transfers with reason code Gifts / Donation to unrelated parties, frequent transfers with reason code off-market sales
9	Alerts for newly opened accounts wherein sudden increase in transactions activities in short span of time and suddenly holding in demat account becomes Zero or account becomes dormant after some time.
10	Other alerts in order to prevent and detect any type of market manipulation activity carried out by the clients.

Based on the above-mentioned themes / parameters, generate the alerts, and review these alerts based on facts and verification of relevant documents including income / Networth as provided by the client. DP Team is required to exercise their independent judgment and take appropriate action to detect any abnormal or suspicious transactions.

C. Obligation of DP regarding client due diligence:

1. To carry out Due-Diligence of the clients on an on-going basis. Based on the documents submitted by the clients and the transactions carried out on the demat accounts, required to carry out the due – diligence and prepare the report based on the suspicious transaction on the demat account and review the same by the independent team other than the report generated.
2. Update the key KYC Parameters of the clients are updated on a period basis as prescribed by SEBI and latest information of the client is updated in depository system. Being the DP, clients are provided the access of entire information through the Company's portal (https://www.agroy.com) and allowed the clients to verify the basic details through the Account Verification Requests of the client. In this Option module, clients are allowed to verify the key KYC parameters as such, Mobile number, Email ID, Address details, Bank Account details registered with the DP Account and Income Range. If the client wanted to make the necessary changes in the above key parameters, they can perform the same which is validated and updated the same after necessary due diligence and also through maker and checker concept by the DP.

D. Reporting the status of alerts generated by DP:

1) Record each alerts / transaction identified based on the above parameters in the register.
2) Review these alerts based on the request of the client and understand the rational of the transaction and obtain the supporting documents wherever required from the clients.
3) Verify the documentary evidence and record its observation for such identified transactions of its clients.
4) With respect to the transactional alerts provided by Depository, ensure that all alerts are reviewed, and status thereof (Verified & Closed / Verified & Reported to Depository) including the action taken is updated within 30 days from the date of alert generated.
5) With respect to the alerts generated at the DP end, report instances with adverse observation, along with details of action taken to Depository within 7 days of the date of identification of adverse observation.

E. Obligation of Compliance Officer and Internal Auditor / Concurrent Auditor:

1. Compliance Officer of the DP is the responsible for supervising the surveillance activities of DP as stipulated with this policy.
2. Compliance Offer prepare the quarterly MIS report and place the same to the Board on the number of alerts pending at the beginning of the quarter, generated during the quarter, processed and acted upon during the quarter and cases pending at the end of the quarter along with the reasons for pendency and action plan for closure. Also, the Board shall be appraised of any exception noticed during the disposal of alerts.
3. Internal Auditor of DP shall review the surveillance policy and its implementation, effectiveness and review the alerts generated during the period of audit, internal auditor shall record the observations with respect to the same in their report.
4. Internal Auditor shall verify the quarterly MIS is prepared and placed before the Board of the DP.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

5. Compliance Officer required to provide the duly approved status of the alerts on a quarterly basis, in the format specified by the Depository within 15 days from the end of the quarter.

In case any further information / Clarification are required in this regard, the compliance officer may be contacted.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

CYBER SECURITY & CYBER RESILIENCE POLICY

Appendix K

Last Review Date: 05-June-2022

INTRODUCTION:

This Cyber Security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

This framework is formed in accordance with the requirements of the SEBI CircularSEBI/HO/MIRSD/CIR/PB/2018/147 ("the circular") dated December 3, 2018.

The objective of this framework is to provide robust cyber security and cyber resilience to the Stockbrokers and depository participants to perform their significant functions in providing services to theholders of securities.

Provisions of the said circular and framing of cyber security and cyber resilience are required to becomplied by all Stock Brokers and Depository Participants registered with SEBI.

Scope

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access ofsystems and information to authorized users, Integrity is the assurance that the information isreliable and accurate, and Availability refers to guarantee of reliable access to the systems andinformation by authorized users). Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is anorganization's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack.

With the view to strengthen and improve Cyber Security and Cyber Resilience framework, the board of directors of the company shall review this policy documents and implementation thereof at least once annually.

POLICY

IDENTIFICATION, ASSESSMENT AND MANAGEMENT OF CYBER SECURITY RISK

The company shall ensure the following steps in order to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems.

IDENTIFICATION OF CRITICAL IT ASSETS AND RISKS ASSOCIATED WITH SUCH ASSETS

The committee and designated officer shall identify the critical assets based on their sensitivity and criticality for business operations, services and data management including various servers, data processing systems, and information technology (IT) related hardware and software etc.

The IT team shall maintain up-to-date inventory of its hardware and systems and the personnel towhom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

PROTECTION OF ASSETS BY DEPLOYING SUITABLE CONTROLS, TOOLS AND MEASURES

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

In order to protect the cyber safety, the company shall ensure the measures which include, however not limited upto:

- Access controls
- Physical Security
- Network Security Management
- Data security
- Hardening of Hardware and Software
- Application Security in Customer Facing Applications
- Certification of off-the-shelf products
- Patch management
- Disposal of data, systems and storage devices
- Vulnerability Assessment and Penetration Testing (VAPT)

The company shall take all such steps to protect assets of the company by deploying suitable controls, tools and measures in conformity with the provisions of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018 and any amendment or substitution thereof. However, the committee and designated officer of the company shall additionally deploy such measures in this respect, as may be warranted from time to time.

DETECTION OF INCIDENTS, ANOMALIES AND ATTACKS THROUGH APPROPRIATE MONITORINGTOOLS/PROCESSES

Necessary steps as may be required to monitor and for early detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission ofdata / information held in contractual or fiduciary capacity, by internal and external parties shall be maintained, appreciated and taken care on.

The security logs of systems, applications and network devices exposed to the internet shall also be, from to time, monitored for anomalies, if any.

The company shall ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, and implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet.

RESPONDING BACK BY TAKING IMMEDIATE STEPS AFTER IDENTIFICATION OF THE INCIDENT, ANOMALY OR ATTACK

The alerts generated from monitoring and detection of systems in order to determine activities that are to be performed to prevent expansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident.

In case of affection of systems by incidents of cyber-attacks or breaches, the company shall ensure timely restoration of the same in order to provide uninterrupted services. The committee and designated officer shall ensure to have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as per regulatory requirements.

With a view to providing quick responses to such cyber-attacks, the committee shall formulate a response plan defining responsibilities and actions to be performed by its employees and support /outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism. Such plan and any modification therein shall be circulated amongst all the employees and support / outsourced staff from time to time.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

RECOVERY FROM INCIDENT(S) THROUGH INCIDENT MANAGEMENT AND OTHER APPROPRIATE RECOVERY MECHANISMS

The company shall take into account the outcomes of any incident of loss or destruction of data or systems and accordingly shall take precautionary measures to strengthen the security mechanism and improve recovery planning and processes.

Periodic checks to test the adequacy and effectiveness of the aforementioned response and recovery plan shall be done.

The technology committee in accordance with the provisions of the said circular and formed hereinafter this framework, shall ensure that this framework considers the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.

COMMUNICATION OF UNUSUAL ACTIVITIES AND EVENTS

IT team of the company under guidance of the committee shall monitor unusual activities and events and shall facilitate communication of the same to designated officer for necessary actions, as may be required.

RESPONSIBILITIES OF EMPLOYEES, MEMBERS AND PARTICIPANTS

In addition to the followings, the employees, members and participants shall be responsible for the duties and obligations as may be entrusted and communicated by the company / committee /designated officer from time to time.

To prevent the cyber attacks, the employees, members and participants shall assist the company to mitigate cyber attacks by adhering the followings:

- To attend the cyber safety and trainings programs as conducted by the company from time to time.
- To endure installation, usage and regular update of antivirus and antispyware software on computer used by them.
- Use a firewall for your Internet connection.
- Download and install software updates for your operating systems and applications as they become available.
- Make backup copies of important business data and information.
- Control physical access to your computers and network components.
- Keep your Wi-Fi network secured and hidden.
- To adhere limited employee access to data and information and limited authority to install software.
- Regularly change passwords.
- Do not use or attach unauthorised devices.
- Do not try to open restricted domains.
- Avoid saving your personal information on computer or any financial data on any unauthenticwebsite.
- To get your computer regularly scanned with anti-virus software.
- Do not release sensitive data of the organization.

Further the company shall ensure that:

- No person by virtue of rank or position shall have any intrinsic right to access confidential data,applications, system resources or facilities.
- Any access to the systems, applications, networks, databases, etc., shall be for a defined purposeand for a defined period. The company shall grant access to IT systems, applications, databasesand networks on a need-to-use basis and based on the principle of least privilege. Such accessshall be for the period when the access is required and should be authorized using strongauthentication mechanisms.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

- An access policy which addresses strong password controls for users' access to systems,applications, networks and databases shall be implemented.
- All critical systems accessible over the internet should have two-factor security (such as VPNs,Firewall controls etc.), as far as possible.
- The company shall ensure that records of user access to critical systems, wherever possible, areuniquely identified and logged for audit and review purposes and such logs would be maintainedand stored in a secure location for a time period not less than two (2) years.
- The company shall be required to deploy controls and security measures to supervise staff withelevated system access entitlements (such as admin or privileged users) to company's criticalsystems. Such controls and measures shall inter-alia include restricting the number of privilegedusers, if any, periodic review of privileged users' activities, disallow privileged users fromaccessing systems logs in which their activities are being captured, strong controls over remoteaccess by privileged users, etc.
- Employees and outsourced staff such as employees of vendors or service providers, who may begiven authorized access to the critical systems, networks and other computer resources, shall besubject to stringent supervision, monitoring and access restrictions.
- An Internet access policy to monitor and regulate the use of internet and internet based servicessuch as social media sites, cloud-based internet storage sites, etc. within the company's criticalIT infrastructure shall be formulated.
- User Management shall address deactivation of access of privileges of users who are leaving theorganization or whose access privileges have been withdrawn.
- Physical access to the critical systems shall be restricted to minimum and only to authorizedofficials. Physical access of outsourced staff / visitors shall be properly supervised by ensuring atthe minimum that outsourced staff / visitors are accompanied at all times by authorizedemployees.
- Physical access to the critical systems shall be revoked immediately if the same is no longerrequired.
- The company will ensure that the perimeter of the critical equipments room, if any, shall bephysically secured and monitored by employing physical, human and procedural controls such asthe use of security guards, CCTVs, card access systems, mantraps, bollards, etc. whereappropriate.
- The company shall establish baseline standards to facilitate consistent application of securityconfigurations to operating systems, databases, network devices and enterprise mobile deviceswithin their IT environment. The LAN and wireless networks shall be secured within the premiseswith proper access controls.
- For algorithmic trading facilities, adequate measures shall be taken to isolate and secure theperimeter and connectivity to the servers running algorithmic trading applications, if any.
- The company shall install network security devices, such as firewalls, proxy servers, intrusiondetection and prevention systems (IDS) to protect their IT infrastructure which is exposed to theinternet, from security exposures originating from internal and external sources.
- Adequate controls shall be deployed to address virus / malware / ransomware attacks. Thesecontrols may include host / network / application based IDS systems, customized kernels forLinux, anti-virus and anti-malware software etc.
- Critical data shall be identified and encrypted in motion and at rest by using strong encryptionmethods. Illustrative measures in this regard are given in Annexure A and B.
- The company shall implement measures to prevent unauthorized access or copying ortransmission of data / information held in contractual or fiduciary capacity. It shall ensure thatconfidentiality of information is not compromised during the process of exchanging andtransferring information with external parties.
- This security policy also covers use of devices such as mobile phones, faxes, photocopiers,scanners, etc., within their critical IT infrastructure, that can be used for capturing andtransmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
- The company shall allow only authorized data storage devices within their IT infrastructurethrough appropriate validation processes.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

- The company shall only deploy hardened hardware / software, including replacing defaultpasswords with strong passwords and disabling or removing services identified as unnecessaryfor the functioning of the system.
- Open ports on networks and systems which are not in use or that can be potentially used forexploitation of data shall be blocked and measures taken to secure them.
- Application security for Customer facing applications offered over the Internet such as IBTs(Internet Based Trading applications), portals containing sensitive or private information andBack office applications (repository of financial and personal information offered by Brokers toCustomers) are paramount as they carry significant attack surfaces by virtue of being availablepublicly over the Internet for mass use. Required measures for ensuring security in suchapplications shall be ensured.
- The company shall ensure that off the shelf products, if any, being used for core businessfunctionality (such as Back office applications) should bear Indian Common criteria certificationof Evaluation Assurance Level 4. The Common criteria certification in India is being provided by(STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and InformationTechnology). Custom developed / in-house software and components need not obtain thecertification, but have to undergo intensive regression testing, configuration testing etc. Thescope of tests shall include business logic and security controls.
- The company establish and ensure that the patch management procedures include theidentification, categorization and prioritization of patches and updates. An implementationtimeframe for each category of patches should be established to apply them in a timely manner.
- The company shall perform rigorous testing of security patches and updates, where possible,before deployment into the production environment so as to ensure that the application ofpatches do not impact other systems.
- Suitable policy for disposal of storage media and systems shall be framed as may be required.The critical data
- / Information on such devices and systems shall be removed by using methodssuch as crypto shredding / degauss / Physical destruction as applicable.
- The company shall formulate a data-disposal and data-retention policy to identify the value andlifetime of various parcels of data.
- The company shall regularly conduct vulnerability assessment to detect security vulnerabilities intheir IT environments exposed to the internet, as and when required.
- The company with systems publicly available over the internet shall also carry out penetrationtests, at-least once a year, in order to conduct an in-depth evaluation of the security posture ofthe system through simulations of actual attacks on its systems and networks that are exposedto the internet.In addition, the company shall perform vulnerability scanning and conduct penetration testingprior to the commissioning of a new system that is accessible over the internet.
- In case of vulnerabilities discovered in off-the-shelf products (used for core business) orapplications provided by exchange empanelled vendors, the company shall report them to thevendors and the exchanges in a timely manner.
- Remedial actions, if required, shall be immediately taken to address gaps that are identifiedduring vulnerability assessment and penetration testing.
- The company shall establish appropriate security monitoring systems and processes to facilitatecontinuous monitoring of security events / alerts and timely detection of unauthorised ormalicious activities, unauthorised changes, unauthorised access and unauthorised copying ortransmission of data / information held in contractual or fiduciary capacity, by internal andexternal parties. The security logs of systems, applications and network devices exposed to theinternet shall also be monitored for anomalies, if any.
- Further, to ensure high resilience, high availability and timely detection of attacks on systemsand networks exposed to the internet, the company shall implement suitable mechanisms tomonitor capacity utilization of its critical systems and networks that are exposed to the internet,for example, controls such as firewalls to monitor bandwidth usage.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

- Alerts, if any, generated from monitoring and detection systems shall be suitably investigated inorder to determine activities that are to be performed to prevent expansion of such incident ofcyber attack or breach, mitigate its effect and eradicate the incident.
- The response and recovery plan of the company shall have plans for the timely restoration ofsystems affected by incidents of cyber-attacks or breaches, for instance, offering alternateservices or systems to Customers. The company shall have the same Recovery Time Objective(RTO) and Recovery Point Objective (RPO) as per regulatory requirements.
- Responsibilities and actions to be performed by company's employees and support / outsourcedstaff in the event of cyber-attacks or breach of Cyber Security mechanism shall be defined.
- Any incident of loss or destruction of data or systems shall be thoroughly analyzed and lessonslearned from such incidents shall be incorporated to strengthen the security mechanism andimprove recovery planning and processes.
- Suitable periodic checks to test the adequacy and effectiveness of the aforementioned responseand recovery plan shall be done.

SUBMISSION OF QUARTERLY REPORTS

Quarterly reports containing information on cyber-attacks and threats experienced, if any, by the company and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants shall be submitted to Stock Exchanges / Depositories, as per statutory requirements /guidelines.

TRAINING AND EDUCATION

The committee and designated officer shall conduct training and educational sessions for employees to make them aware on building Cyber Security and basic system hygiene awareness, to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts, including to outsourced staff, vendors, if any, and shall take all such steps as may be deemed appropriate by them in this respect.

SYSTEMS MANAGED BY VENDORS

Whenever the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of the company are managed by vendors and the company may not be able to implement some of the aforementioned guidelines directly, the company shall, from time to time, instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

SYSTEMS MANAGED BY MIIS

Wherever the applications are offered to customers over the internet by MIIs (Market Infrastructure Institutions), for eg.: NSE's NOW, BSE's BEST etc., the responsibility of ensuring Cyber Resilience on those applications reside with the MIIs and not with the company. In such case, the company is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc.

PERIODIC AUDIT

The company shall arrange to have its systems audited on an annual basis by a CERT-IN empanelled auditor or an independent DISA/ CISA / CISM qualified auditor to check compliance with the above areas and shall submit the report to Stock Exchanges / Depositories along with the comments of the Board/ committee / any committee thereof within three months of the end of the financial year.

Enclosures:

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Annexure A: Illustrative Measures for Data Security on Customer Facing Applications Annexure B: Illustrative Measures for Data Transport Security
Annexure C: Illustrative Measures for Application Authentication Security

Annexure A
Illustrative Measures for Data Security on Customer Facing Applications

1. Analyse the different kinds of sensitive data shown to the Customer on the frontend application to ensure that only what is deemed absolutely necessary is transmitted and displayed.
2. Wherever possible, mask portions of sensitive data. For instance, rather than displaying the full phone number or a bank account number, display only a portion of it, enough for the Customer to identify, but useless to an unscrupulous party who may obtain covertly obtain it from the Customer's screen. For instance, if a bank account number is "123 456 789", consider displaying something akin to "XXX XXX 789" instead of the whole number. This also has the added benefit of not having to transmit the full piece of data over various networks.
3. Analyse data and databases holistically and draw out meaningful and "silos" (physical or virtual)into which different kinds of data can be isolated and cordoned off. For instance, a database with personal financial information need not be a part of the system or network that houses the public facing websites of the Stock Broker. They should ideally be in discrete silos or DMZs.
4. Implement strict data access controls amongst personnel, irrespective of their responsibilities, technical or otherwise. It is infeasible for certain personnel such as System Administrators and developers to not have privileged access to databases. For such cases, take strict measures to limit the number of personnel with direct access, and monitor, log, and audit their activities. Take measures to ensure that the confidentiality of data is not compromised under any of these scenarios.
5. Use industry standard, strong encryption algorithms (eg: RSA, AES etc.) wherever encryption is implemented. It is important to identify data that warrants encryption as encrypting all data is infeasible and may open up additional attack vectors. In addition, it is critical to identify the right personnel to be in charge of, and the right methodologies for storing the encryption keys, as any compromise to either will render the encryption useless.
6. Ensure that all critical and sensitive data is adequately backed up, and that the backup locations are adequately secured. For instance, on servers on isolated networks that have no public access end points, or on-premise servers or disk drives that are off-limits to unauthorized personnel. Without up-to-date backups, a meaningful recovery from a disaster or cyber-attack scenario becomes increasingly difficult.

Annexure B
Illustrative Measures for Data Transport Security

1. When an Application transmitting sensitive data communicates over the Internet with the Stock Brokers' systems, it should be over a secure, encrypted channel to prevent Man-In-The-Middle(MITM) attacks, for instance, an IBT or a Back office communicating from a Customer's web browser or Desktop with the Stock Brokers' systems over the internet, or intra or interorganizational communications. Strong transport encryption mechanisms such as TLS (Transport Layer Security, also referred to as SSL) should be used.
2. For Applications carrying sensitive data that are served as web pages over the internet, a valid, properly configured TLS (SSL) certificate on the web server is mandatory, making the transport channel HTTP(S).
3. Avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc.

Annexure C
Illustrative Measures for Application Authentication Security

1. Any Application offered by Stock Brokers to Customers containing sensitive, private, or criticaldata such as IBTs, SWSTs, Back office etc. referred to as "Application" hereafter) over theInternet should be password protected. A reasonable minimum length (and no arbitrarymaximum length cap or character class

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

requirements) should be enforced. While it is difficult toquantify password "complexity", longer passphrases have more entropy and offer bettersecurity in general. Stock Brokers should attempt to educate Customers of these best practices.

2. Passwords, security PINs etc. should never be stored in plain text and should be one-way hashedusing strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed tostorage. It is important to use one-way cryptographic hashes to ensure that stored passwordhashes are never transformed into the original plaintext values under any circumstances.
3. For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used(hardware or software cryptographic tokens, VPNs, biometric devices, PKI etc.). In case of IBTsand SWSTs, a minimum of two-factors in the authentication flow are mandatory.
4. In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used.
5. After a reasonable number of failed login attempts into Applications, the Customer's account can be set to a "locked" state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation, for instance, a cryptographically secure unique link that is sent to the Customer's registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the Customer's registered mobile number, or manually by the Broker after verification of the Customer's identity etc.
6. Avoid forcing Customers to change passwords at frequent intervals which may result in successive, similar, and enumerated passwords. Instead, focus on strong multi-factor authentication for security and educate Customers to choose strong passphrases. Customers may be reminded within reasonable intervals to update their password and multi-factor credentials, and to ensure that their out-of-band authentication reset information (such as email
7. and phone number) are up-to-date.
8. Both successful and failed login attempts against a Customer's account may be logged for a reasonable period of time. After successive login failures, it is recommended that measures such as CAPTCHAs or rate-limiting be used in Applications to thwart manual and automated brute force and enumeration attacks against logins.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

ACCESS CONTROL POLICY

Appendix L

Last Review Date: 05-June-2022

PURPOSE

To ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures.

SCOPE

This policy is applicable to all departments and users of Company resources and assets.

POLICY

Account Management

IT Department shall:

a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.
b. Assign account managers for information system accounts.
c. Establish conditions for group and role membership.
d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
e. Require approvals by system owners for requests to create information system accounts.
f. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.
g. Monitor the use of information system accounts.
h. Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.
i. Authorize access to the information system based on a valid access authorization or intended system usage.
j. Review accounts for compliance with account management requirements once in every three months.
k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
l. Employ automated mechanisms to support the management of information system accounts.
m. Ensure that the information system automatically disables temporary and emergency accounts after usage.
n. Ensure that the information system automatically disables inactive accounts after 15 days of inactivity.
o. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

ACCESS ENFORCEMENT

IT Department shall:

a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

INFORMATION FLOW ENFORCEMENT

IT Department shall:

a. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

SEPARATION OF DUTIES

IT Department shall:

a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.
b. Define information system access authorizations to support separation of duties.

LEAST PRIVILEGE

IT Department shall:

a. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
b. Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.
c. Require that users of information system accounts, or roles, use non-privileged accounts or roles, when accessing non-security functions.
d. Restrict privileged accounts on the information system to system administrators only.
e. Ensure that the information system audits the execution of privileged functions.
f. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

UNSUCCESSFUL LOGON ATTEMPTS

IT Department shall ensure that the information system:

a. Enforces a limit of consecutive invalid logon attempts by a user.
b. Locks the account/node automatically until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

SYSTEM USE NOTIFICATION

IT Department shall ensure that the information system:

a. Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance and states informing that:
    1. Users are accessing a company's information system.
    2. Information system usage may be monitored, recorded, and subject to audit.
    3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.
    4. Use of the information system indicates consent to monitoring and recording.
    5. There are no rights to privacy.
b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.
c. For publicly accessible systems, the IT Department shall ensure that the information system:
    1. Displays system use information, before granting further access.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
3. Includes a description of the authorized uses of the system.

SESSION LOCK

IT Department shall ensure that the information system:

a. Prevent further access to the system by initiating a session lock after 30 minutes of inactivity or upon receiving a request from a user.
b. Retain the session lock until the user re-establishes access using established identification and authentication procedures.
c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

SESSION TERMINATION

IT Department shall:

a. Ensure that the information system automatically terminates a user session after 2 hours of inactivity.

PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

IT Department shall:

a. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.
b. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

REMOTE ACCESS

IT Department shall:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
b. Authorize remote access to the information system prior to allowing such connections.
c. Ensure that the information system monitors and controls remote access methods.
d. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
e. Ensure that the information system routes all remote accesses through a specified managed network access control point to reduce the risk for external attacks.
f. Authorize the execution of privileged commands and access to security-relevant information via remote access only for system administration needs.
g. Document the rationale for such access in the security plan for the information system.

WIRELESS ACCESS

IT Department shall:

a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
b. Authorize wireless access to the information system prior to allowing such connections.
c. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

ACCESS CONTROL FOR MOBILE DEVICES

IT Department shall:

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.
b. Authorize the connection of mobile devices to organizational information systems
c. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices.

USE OF EXTERNAL INFORMATION SYSTEMS

IT Department shall:

a. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
    i. Access the information system from external information systems.
    ii. Process, store, or transmit organization-controlled information using external information systems.
b. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization
    i. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.
    ii. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

INFORMATION SHARING

IT Department shall:

a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information.

PUBLICLY ACCESSIBLE CONTENT

IT Department shall:

a. Designate individuals authorized to post information onto a publicly accessible information system.
b. Train authorized individuals to ensure that publicly accessible information does not contain non-public information.
c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that non-public information is not included.
d. Review the content on the publicly accessible information system for non-public information once in 3 months and removes such information, if discovered.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) or Chief Executive Officer (CEO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

IT SYSTEMS HARDENING POLICY

Appendix M

Last Review Date: 05-June-2022

PURPOSE

Hardening is the process of securing a system by reducing its surface of vulnerability. By the nature of operation, the more functions a system performs, the larger the vulnerability surface.

Most systems perform a limited number of functions. It is possible to reduce the number of possible vectors of attack by the removal of any software, user accounts or services that are not related and required by the planned system functions. System hardening is a vendor specific process, as different system vendors install different elements in the default install process.

The possibility of a successful attack can be further reduced by obfuscation. By making it difficult for a potential attacker to identify the system being attacked the attack can not easily exploit known weaknesses.

SCOPE

This policy applies to all components of the information technology infrastructure and includes:
 Computers Servers Application Software Peripherals Routers and switches Databases Telephone Systems

All staff within the IT Department must understand and use this policy. IT staff are responsible for ensuring that the IT infrastructure is hardened and that any subsequent changes to systems do not affect the hardening of systems.

POLICY

Hardening Process
All new systems will undergo the following hardening process:

1. Install System - Install the systems as per the vendor's instructions.
2. Remove Unnecessary Software - Most some systems come with a variety of software packages to provide functionality to all users. Software that that is not going to be used in a particular installation should be removed or uninstalled from the system.
3. Disable or Remove Unnecessary Usernames - Most systems come with a set of predefined user accounts. These accounts are provided to enable a variety of functions. Accounts relating to services or functions which are not used should be removed or disabled. For all accounts which are used the default passwords should be changed. Consideration should be given to renaming predefined accounts if it will not adversely affect the system.
4. Disable or Remove Unnecessary Services - All services which are not going to be used in production should be disabled or removed.
5. Patch System - The system should be patched up to date. All relevant service packs and security patches should be applied.
6. Perform Vulnerability Scan - The system should be scanned with a suitable vulnerability scanner. The results of the scan should be reviewed and any issues identified should be resolved.
7. Vulnerabilities - If there are no significant vulnerabilities the system can be prepared for live use.
8. Install Anti-Virus and Anti-Malware - A suitable anti-virus and anti-malware package should installed on the system to prevent malicious software introducing weaknesses in to the system.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

9. Configure Firewall - If the system can run its own firewall then suitable rules should be configured on the firewall to close all ports not required for production use.
10. Production System - The system is now ready for production use.

Hardening Requirements

1. Only software that has been approved for use by the IT department may be installed on the organisation's computing devices.
2. Non-essential software applications and services will be uninstalled or disabled as appropriate.
3. Servers, PC's and laptops will be configured to prevent the execution of unauthorised software.
4. Vulnerability scanning and inventory scanning software will be configured to automatically uninstall unauthorised software.
5. Bios passwords will be implemented on all PCs and laptops to protect against unauthorised changes.
6. The boot order of PC's and laptops will be configured to prevent unauthorised booting from alternative media.
7. All PC's and laptops will be built from a standard image. Any change to the standard image must be supported by a business case.
8. Access to the local administrator account will be restricted to members of IT Department to prevent the installation of unauthorised software and the modification of security software and controls.
9. Default passwords will be changed following installation and before use in a production environment.
10. All PC's and servers will be protected by anti-virus and anti-spyware software. The anti-virus and anti-spyware software will be configured to automatically download the latest threat databases.
11. A local firewall will be installed on all PC's and laptops. The firewall will be configured to only allow incoming traffic on approved ports and from approved sources.
12. The use of removable media will be controlled. Removable media will be controlled by endpoint protection software.
13. All servers must pass a vulnerability assessment prior to use. The servers will be scanned using the organisations vulnerability scanning tools. All network and operating system vulnerabilities will be rectified prior to use.
14. Public facing servers will be further hardened by obfuscation. The headers on web servers and email servers will be changed so that it is not immediately apparent what software they are running.
15. All devices on the organisation's network will be scanned for vulnerabilities every 3 months. Any issues identified will be reviewed and rectified as appropriate.
16. All devices on the organisation's network will patched in accordance with the Technical Vulnerability and Patch Management Policy.

Enforcement

1. If any member of IT staff is found to have breached this policy, they may be subject to disciplinary action.
2. Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

IT INCIDENT MANAGEMENT POLICY

Appendix N

Last Review Date: 05-June-2022

PURPOSE

The purpose of this policy is to ensure that the Company reacts appropriately to any actual or suspected security incidents relating to information systems and data.

The objective of this policy is to ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody and infrastructure.

SCOPE

All users shall understand and adopt use of this policy and are responsible for ensuring the safety and security of the Company's systems and the information that they use or manipulate.

POLICY

This policy shall to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident. An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system. Changes to information or data or system hardware, firmware, or software characteristics without the organization's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorized use of a system for the processing or storage of data by any person
- Intentional or unintentional damage to access control and surveillance systems
- External or foreign body trying to gain unauthorized access to Company's information systems

Responsibilities and Procedures

- Preparation shall involve identification of resources needed for incident handling and having trained individuals ready to respond, and by developing and communicating a formal detection and reporting process.
- Effective, appropriate communication at all levels of an organization shall be implemented for limiting the impact of security events.
- Who can access data relating to an incident under what circumstances and what auditing is required to document the access shall be specified.
- Records of Data retention of non-incident related log data and data preserved during investigation of an incident shall be maintained.
- Computer security professionals shall perform some examination and analysis to determine whether an incident is serious enough to report to law enforcement under the supports of IT Act 2000 (amendment 2008)

Reporting Information Security Events

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

- Designing of an effective means of the detection of incidents shall be implemented using both trained users and trained system administrators, and various technical controls.
- All members of the community shall be trained and comfortable regarding:
  - procedures for reporting failures, weaknesses, and suspected incidents
  - methods to recognize and detect problems with security protections
  - how to escalate reporting appropriately
- Technical controls shall be implemented for the automated detection of security events, coupled with as near real-time reporting as possible, to investigate and initiate immediate responses to problems.

Reporting Information Security Weaknesses

- An effective approach of tools shall be used for analysis to help manage intrusion detection systems and summarize the data.
- Information security events shall be reported through appropriate management channels as quickly as possible
- Staffs and third party service providers using the organization's information system and services shall note and report any observed or suspected information security weaknesses in systems or services.

Response to information security incidents

- Information security incidents shall be responded to in accordance with the documented procedures.
- All the security incidents shall be reported to the concerned authority as per the procedure.

Learning from Information Security Incidents

- Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
- The information must be collated and reviewed on a regular basis by Information Security team and any patterns or trends identified.
- Any changes to the process made as a result of the Post Incident Review shall be formally noted.

Collection of Evidence

- The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.
- If an incident may require information to be collected for an investigation, strict rules must be adhered to.
- The collection of evidence for a potential investigation shall be approached with care.
- Internal Audit team shall be contacted immediately for guidance and strict processes must be followed for the collection of evidence.

ENFORCEMENT

- This document applies to all Departments of the Company and third party service providers of the Company who use the Company's IT facilities and equipment, or have access to customer information or the Company's information.
- Any staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

INTERNET ACCESS AND USE POLICY

Appendix O

Last Review Date: 05-June-2022

PURPOSE

Our internet usage policy outlines our guidelines for using our company's internet connection, network and equipment. We want to avoid inappropriate or illegal internet use that creates risks for our company's legality and reputation.

SCOPE

This internet access and usage policy applies to all our employees, contractors, volunteers and partners who access our network and computers.

POLICY

What is appropriate employee internet usage?

Our employees are advised to use our company's internet connection for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our confidentiality and data protection policy.

Employees should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

What is inappropriate employee internet usage?

Our employees mustn't use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask IT Support team.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

Our company may install anti-virus and disk encryption software on our company computers. Employees may not deactivate or configure settings and firewalls without managerial approval.

We won't assume any responsibility if employee devices are infected by malicious software, or if their personal data are compromised as a result of inappropriate employee use.

Company-issued equipment

We expect our employees to respect and protect our company's equipment. "Company equipment" in this computer usage policy for employees includes company-issued phones, laptops, tablets and any other electronic equipment, and belongs to our company.

We advise our employees to lock their devices in their desks when they're not using them. Our employees are responsible for their equipment whenever they take it out of their offices.

Email

Our employees can use their corporate email accounts for both work-related and personal purposes as long as they don't violate this policy's rules. Employees shouldn't use their corporate email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorized advertisements or solicitation emails.
- Sign up for a competitor's services unless authorized.

Our company has the right to monitor corporate emails. We also have the right to monitor websites employees visit on our computers.

ENFORCEMENT

Employees who don't conform to this internet access and usage policy will face disciplinary action. Serious violations will be cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

BUSINESS CONTINUTY PLAN AND DISASTOR RECOVERY POLICY

Appendix P

Last Review Date: 05-June-2022

PURPOSE

The Company is in the business of share and stock business and distribution of products. The entire business module is the function of proper human resource utilization / management and the state of art of technology / I.T. infrastructure amongst others.

SCOPE

This policy applies to all our employees, contractors, volunteers and partners who access our network and computers.

POLICY

Recovery, resumption and maintenance

Share and trading business is the key activities to the organization. In order to this business the company has implemented various CTCL, software in addition to NEAT / BOLT System for trading with NSE and / or BSE. Respective vendors make constant upgradations and implementations accordingly. Trained human resources are employed for the purpose.

A detailed policy for disaster recovery is separately made and successfully implemented in the organization, which includes DRP, changes Management amongst others.

a) Data Recovery - A proper Data Backup policy stating the recovery, resumption and restoration of the data is adapted and following by the company. The company ensures the restoration of data at intervals to ensure business continuity in time of crisis.
b) System & Hardware - The Company claim to have a techno-savy environment. As management policy it keeps on investing in upgraded hardware's and software's are required from time to time.
c) Monetary Loss - Increasing complexities in the financial business environment attracts new risk to the business model. The company always looks forward for implementation of new software's to counter such monetary losses.
d) Offsite - The company has a vision of PAN India network and has already opened quite a few branches and a few more are in process. Mumbai Data Center (CDAC) has been used with a view to function as an offsite to keep the business continuity in cases of emergencies when the HO (i.e. Delhi office) goes down. Company has an 'Incident Response Policy' that explains the plan.
e) Environmental - Flood, Earthquakes, Riot, Fire etc are the threats for which the company has continuity plans.
    - Long Term Plans
        - Offsite operations from Mumbai
    - Continuous Plans
        - Insurance Policies
        - Maintenance of server / software.
        - Backup

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

f) Recovery Plans - The biggest challenge is the recovery of the business in times of crisis. The crisis may come for the following factors:
   - Data Backup – Please refer to backup policy.
   - Server- Maintenance contracts are given.
   - Nodes – Front and user – An in house efficient team is there to look after
   - Software's – Front and back –Appropriate contracts are made with the vendors to ensure smooth functioning.

Business Objectives

Prioritization of financial services to the best of satisfaction of its clients and realization of own set targets are the prime objectives of the company.

In the existing dynamic market situation the company need to constantly vouch for the latest development in the market environment with regards to available models of business and the requisite I.T and human resources.

Accordingly the company has evolutes its paradigm from the conventional self centered business to break into retail segment. Similarly on the I.T front various new software's have been introduced onto the system.

Regular Updates to the BCP

The company has a technology savy senior management team who understand the entire prospects of the business viz-a-viz technological changes, understanding the critical operation, business dynamics, human resources management, general administration and all other related matters.

The said senior management team constantly interacts on the evolution of the BCP.

Proper Risk assessment, implementation and management

Assessing and managing the risk is the key function of the business.
Any miss-assessment of the risk for transaction done whether for transaction done whether for self or for clients may have adverse impact on the company business. Therefore, the proper risk assessment for all the processes is very important. The business models are accordingly formulated.

Once the models are formulated proper implementation and management of the same is done with available I.T. human resource in light of the relevant policies of the company formulated for the purpose.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

PATCH MANAGEMENT POLICY

Appendix Q

Last Review Date: 05-June-2022

PURPOSE

The goal of vulnerability and patch Management is to keep the components that form part of information technology infrastructure (hardware, software and services) up to date with the latest patches and updates.

Vulnerability and patch management is an important part of keeping the components of the information technology infrastructure available to the end user. Without regular vulnerability testing and patching, the information technology infrastructure could fall foul of problems which are fixed by regularly updating the software, firmware and drivers. Poor patching can allow viruses and spyware to infect the network and allow security weaknesses to be exploited.

This policy defines the procedures to be adopted for technical vulnerability and patch management.

SCOPE

This policy applies to all components of the information technology infrastructure and includes:-

- Computers
- Servers
- Application Software
- Peripherals
- Routers and switches
- Databases
- Storage

All staff within the IT Department must understand and use this policy. IT staff are responsible for ensuring that the vulnerabilities within the IT infrastructure are minimized and that the infrastructure is kept patched up to date.

All users have a role to play and a contribution to make by ensuring that they allow patches to be deployed to their equipment.

RISKS

Without effective vulnerability and patch management there is the risk of the unavailability of systems. This can be caused by viruses and malware exploiting systems or by out of date software and drivers making systems unstable.

POLICY

The organization's IT infrastructure will be patched according to this policy to minimize vulnerabilities.

Identifying Patches to be applied

1. The organization's anti-virus server will be configured to automatically down load the latest virus and spyware definitions.
2. Windows patch management tools will be utilized to automatically download the latest Microsoft security patches. The patches will be reviewed and applied as appropriate.

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024

3. Notifications of patches from application and database vendors will be reviewed and the patches applied as appropriate. Where notifications are not automatically sent, the suppliers website will be reviewed on a regular basis.
4. The websites of the suppliers of servers, PC's, printers, switches, routers and peripherals will be reviewed to determine the availability of firmware patches.
5. Missing patches identified will be implemented as appropriate. Any weaknesses identified will be rectified.
6. Any system updates/patches for Linux operating systems must be done by the relevant service provider, tested and implemented.
7. For all updates on Linux operating systems, the Change control process must be followed, to ensure successful completion of update and minimize any problems that might occur.

Types of Patches

The following patches will be implemented on the different information infrastructure types.

Type	**Patch**
Server/Computer	Drivers / firmware
Operating System	Service Packs
Application software	Service packs, feature packs
Router and switches	Firmware
Printers	Drivers / firmware
Scanners	Drivers / firmware
Anti-virus / Anti-spyware	Data file / Virus definition update

Grievances: customercare@agroy.com
Regd. Office: A-21 Kailash Colony, New Delhi 110048
Call: +91 11 46007600 Fax: +91 11 46007611
Compliance Officer: Ashish Kumar Gupta
Email: ashish.gupta@agroy.com **Mobile: 9312211839**

AGROY Finance and Investment Ltd.
SEBI Reg.No.: NSE/BSE/MCX INZ000185530
CDSL: IN-DP-513-2020 (DP ID 12060700)

Prepared by: Tushar Agarwal (Designated Director)
Approved by: Board of Directors
Approved on: 03-Jun-2024