

DATA ACCESS AND DATA PROTECTION POLICY

1. Overview

Computer Age Management Services Ltd. (CAMS) has been appointed by Pension Fund Regulatory and Development Authority (PFRDA) as the third Central Recordkeeping Agency (CRA), for National Pension System (NPS).

CAMS has also been certified for Information Security under, ISO-27001 and since it handles and has access to Sensitive Personal Data or Information (SPDI), it has the greater role to ensure that access to sensitive data are given appropriately only to the authorized users and it implements suitable controls to restrict access to the data.

Accordingly, this policy has been framed to provide the guidelines for Data Access and also for Data Protection.

2. Objective / Purpose

The purpose of this Policy is to specify the terms under which users are provided access to the Data and to define the steps for protection of the database, servers and the specified data from unauthorized access. In adherence to the above objective, this policy defines the following:

1. Process for providing access to the applications/data/database/servers maintained by CAMS
2. The approved mode of access to the applications/data/database/servers
3. The Roles and responsibilities of data users both internal & external
4. Protocols to be followed while providing such access
5. Monitoring and Audit Mechanism for fulfilling the objectives and purpose of the Policy
6. Setting out the principles of data protection and to provide a managed framework for fulfilling business needs, accountability and legal responsibilities

7. Ensuring provision of adequate level of data protection to meet the regulatory and Information security standards

3. Scope

Applicable to all internal users/employees, intermediaries and subscribers who have / propose to have access to the applications/data/database/servers.

4. High-level Policy Statement

a) CAMS, on behalf of PFRDA, collects, records and uses personal data of the subscribers including past, present and prospective in order to carry on its business as per contractual obligation and meet its regulatory requirements effectively. We recognise that integrity and protection from unauthorised access / usage of personal data is very important to successful operations and to maintaining subscriber's confidence in CAMS.

b) Any personal data that we collect record or use in any way whether it is held on paper, on computer or other electronic media will have appropriate safeguards applied to it to ensure that we comply with our regulatory obligations of confidentiality and privacy.

c) Any sensitive information as provided by the subscribers or through their intermediary engaged by the Regulator for processing, stored or processed under lawful contract or otherwise, both historic and ongoing are being used strictly for the purpose for which it has been collected (i.e.) order to carry on its business and meet clients' requirements and deliverables effectively.

d) The above information collected is stored in a secure manner which compiles with ISO 27001 Standards. CAMS aspires to adhere to certain generally accepted principles of data protection, to the extent these CAMS's control as intermediaries.

These general principles state that personal data must be

- Fairly and lawfully collected and processed
- Processed for limited purposes and not in any other way which would be incompatible with those purposes
- Accurate and kept up to date
- Not kept for longer than is necessary

- Kept secure

To meet the requirements of the principles, following process and controls are adhered:

- Observe ethical practices regarding the fair collection and use of personal data
- Collect and process appropriate personal data only to the extent that we are obliged by contract or to comply with any Legal requirements
- Ensure the quality of personal data used
- Hold the data only as long as required by contract or by Law
- Take appropriate security measures to safeguard personal data

e) Personal / Institutional Data shall be classified in accordance with its sensitivity, level of confidentiality needs, legal requirements, and minimum standard protection/s required for the data before access is granted.

f) Electronic Access to data shall be provided to the users on need-to-know basis, depending upon the business, functions, process, legal, statutory and audit requirements. All such access shall be controlled by reasonable measures to prevent access by unauthorized users.

g) Data Users must responsibly use the data for which they have been given access including using the data only for its intended purpose and respecting the privacy of other clients. Data Users must maintain the confidentiality of data in accordance with all applicable Laws & CAMS Privacy Policy. Authorized access to Data does not imply authorization for copying, further dissemination of data, or any use other than the use for which the data user was authorized.

5. Definitions

a) **Access** - Flow of information between a store of data and a user, system, or process. A user, system, or process is considered to have access to data if it has one or more of the following privileges: the ability to read or view the data, update the existing data, create new data, delete data or the ability to make a copy of the data. Access can be provided either on a continual basis or, alternatively, on a one-time or ad hoc basis. Transferring any

data from one party to another in any medium is tantamount to permitting access to those data.

b) **Data (including Personal Data)** - Those data, regardless of format, maintained by CAMS for reference or use by CAMS's regulatory / contractual obligations in providing its CRA services. Personal Data does not include data that is personal property of an employee of CAMS, research data, or data created and/or kept for their own use.

c) **Sensitive Personal Data or Information (SPDI)** - Those Data that contain information that can be classified as either "sensitive" or "restricted". SPDI includes Personal Data that are personally identifiable in nature and contain Personal Account Numbers, Unique identification numbers, or other financial account numbers, NPS transaction information, or protected financial information records of subscribers, PoPs (Point-of-Presence), PoP Service Providers, Subscriber Bank Account details provided either as part of the application submitted by the subscriber or based on written request such as change of bank account, Payment instrument details provided as part of application at the time of onboarding or as proof for carrying out change of bank account Generation and storing password (PIN) in encrypted form based on the request from the subscriber, Physical, physiological and mental health condition, Sexual orientation, and any other information as deemed fit in terms of any Legislations / PFRDA regulations or guidelines / ISO Standards

d) **The words - User, Data User, User Entity, Customer,** refers to the person(s) that has been authorized to access data for the performance of his/her duties, an intermediary or user consuming services / facilities provided through any of the CAMS software applications / platforms to

1. Avail CAMS's services under a contractual agreement

2. Pension Fund Managers, PoPs, PoP SPs, & other intermediaries (all includes their authorized signatories, officers, employees, so on) associated with CAMS directly and indirectly and those who are given access to the services offered under various electronic and non-electronic forms and shall mean and include both singular and plural.

e) **Terms and Conditions** - shall mean the terms and conditions as contained in this policy for providing data access or in the terms and conditions subject to which data

access has been provided to any of its software applications / platforms including third party applications and such terms and conditions can be modified from time to time by CAMS.

f) **Confidential Information** - refers to information obtained by the user, through/from CAMS, for the effective availment of Services or Online transaction services

g) **Internet** -refers to the network of computers / mobile phones / other electronic devices which share and exchange information. The Internet is at once a worldwide broadcasting capability, mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers / mobile phones / other electronic devices capable of accessing the Internet without regard for geographic location.

h) **Online Services** - CAMS's Service which provides access to account information, products and other services as advised by CAMS from time to time to Customers through the Internet.

i) **Customer** - refers to any person who subscribes to NPS with CAMS as CRA

j) **Account** - refers to the Customer's National Pension System (NPS) account / User login account for information services or any other type of account so designated by CAMS NPS to be eligible account(s) for operations through the use of CAMS applications.

k) **Browser Based Service(s) or generally Services** - refers to all CAMS offered services through one or more of its software applications/platforms, including third party applications, as CAMS may decide from time to time. CAMS reserves the right to decide the type of services which may be offered on each platform / account and what type of access / security protocols to be complied with for securing such services. The extent and / or type of services offered may differ from customer to customer. These facilities shall be offered in a phased manner at the discretion CAMS. CAMS may also make additions / deletions to the services offered through its software applications at its sole discretion.

l) **CAMS** means M/s. Computer Age Management Services Private Limited, a company registered under the Companies Act, 1956, having its registered office at No.10 (Old No.178), M. G. R. Salai, Nungambakkam, Chennai – 600 034 (hereinafter referred to as

“CAMS”, which term shall, unless it be repugnant to the context or meaning thereof, be deemed to include their respective successors)

m) **CRA** refers to a Central Recordkeeping Agency registered with PFRDA

n) **PoP (Point of Presence)** refers to an entity appointed for the purposes of the distributing the NPS products that are managed by Pension Fund Managers.

o) **NPS** refers to National Pension System registered with PFRDA and NPS Trust.

6. Terms & Conditions applicable to every mode of Data Access

Users who are having electronic access to CAMS database / servers directly or indirectly shall ensure adequate safeguards including the following:

a) **Security & Access Control:**

1. User entity must be aware that User's and CAMS network are interconnected through the Internet and / or other Private Networks where applicable.
2. User entity must ensure that all such points of interconnection are protected with appropriate means of Access Control, which are adequate and capable of protecting the network against unauthorized access.
3. User entity shall keep such access control measures current and shall not remove or reconfigure so as to significantly increase the risk of unauthorized access.
4. User entity shall always ensure availability of Virus Detection and Control measures throughout its network and in particular in the machines which will be used to access CAMS Network/application, and the same shall be kept current and updated.
5. User entity shall ensure unauthorized access is not taking place in its network and if it comes across any evidence of such unauthorized access, the entity should notify CAMS of such unauthorized access.
6. Wherever administrative rights are provided to the User Entity, enabling the entity to carry out addition, modification and deletion of the users, and user entity provides such access to its employees, in the event of termination of the services of the concerned employee, the user entity should ensure that the access for such

employee is disabled. In the absence of the same, user entity will assume entire responsibility for any mis-use / non-compliance.

7. In the interest of data security, should CAMS observe or apprehend a risk of unauthorized access, CAMS will, at its sole discretion, terminate access at CAMS' end with a reasonable notice to the user entity.
8. User entity shall preserve the login credentials issued to their users in safe manner and keep the same protected. In case of loss/theft or any identified misuse of any account, user entity shall inform CAMS in writing immediately.
9. Wherever required CAMS would allot a user ID and communicate the password to the users / user entity in secured manner and users are required to change the password assigned by CAMS during first log-in and thereafter it must be changed by the users periodically but not later than 90 days. If the application provides for , password which is self-definable / configurable and in such instances, the passwords to be reset periodically and users must ensure that it is safe-guarded appropriately at their end and should not be shared with others
10. In addition to User-ID and Password, CAMS may, at its discretion, require Users / User entities to adopt such other means of authentication including but not limited to digital certification and / or smart cards.
11. Users / User entity shall not attempt or permit others to attempt accessing the account information stored in the computers of CAMS through any means other than designated means.

b) CAMS Commitments

1. CAMS will take utmost care in processing, storing and maintaining such information so that such sensitive and personal information shall not get exposed to any unrelated third party(ies) and used for specific & associated purpose for which such information is collected. CAMS has implemented all required processes and controls as required under local data protection & privacy Laws (Information Technology Act, 2000 & amendments thereof from time to time) and will continue to abide by all such data protection & privacy Laws as notified by Government of India from time to time.
2. CAMS extend all such co-operation to the subscribers , regulators, PoPs and other PFMs, as is necessary for effective and smooth subscriber servicing.

3. CAMS have appropriate protocols, processes and controls for its activities and for entities who wish to connect with the database of CAMS electronically. Those who also connect with CAMS electronically should follow the Data protection guidelines (prescribed as part of this document and in the same manner or more stringent manner without diluting the basic requirements) to maintain the confidentiality, integrity and availability of the data or information.
4. We shall reveal only such information to external authorities as may be found relevant and necessary to comply with the applicable Laws of the land. We may also provide the information to third party service providers like Regulator and NPS Trust/ PFMs / Trustee Bank/ PoPs / Service Providers / Call-centres / Custodian and such other entities/persons to ensure smooth functioning of the activities as may be required to be performed by these entities under the Laws applicable to them.
5. CAMS will also ensure that all personal and sensitive personal data is held securely and protected from destruction, loss, unauthorised access and disclosure. Appropriate obligations are incorporated into contracts with third parties.
6. CAMS encourages its third-party service providers, data recipients to have similar standards of Information Security in their process to adhere the Data protection policy of CAMS or any other suitable standards / guidelines

c) Data User Commitments

1. User / User Entity desiring to invest/transact in NPS scheme are required to familiarize with the data protection / privacy guidelines of Indian Laws and such defined policy of the NPS Trust / PFRDA / CAMS (CRA) with respect to collection, use, disclosure and transfer of information by then NPS Account /PoPs/ PoP SPs and/or affiliate(s), which operates through various branch(es) of its own and/or its relationship managers, various websites and other services including but not limited to delivery of information and content via any mobile or internet connected devices or otherwise (collectively referred to as "Services").
2. User / User Entity agrees and acknowledges that as part of account opening and transaction process, PoP/PoP SP is collecting required information (including personal and sensitive information) from the subscriber(s) through various sources and processed by CAMS (CRA – Central Recordkeeping Agency) and hence such data is stored, maintained and used by the CRA for seamless processing of

transactions initiated by the subscribers. During such processing, data is shared with various stakeholders including PFMs, Distributors, PoPs and Courier agencies, payment service providers, printers, Depositories, Exchanges and so on. CRA will also carry-on data mining using available information for product enhancement, service delivery excellence, digital initiatives, sending email communication on various developments or for regulatory purpose and so on. There are times, where additional information is collected, or 2. existing information are changed, including information collected through third parties like KRAs, etc. and these shall also be used for the above said purposes. User / User Entity should take note of such process and explicitly understand such necessity for flow of information with various stakeholders.

3. User / User Entity, by choosing to invest in the National Pension System and / or having electronic access to CAMS Database / server, is construed to have provided explicit consent to CAMS CRA and other entities engaged by CRA to process subscriber data in their roles as per existing & prospective processes determined by CRA from time to time.
4. CAMS will advise the User/User Entity from time to time the Internet software such as Browsers, which are required for using its Internet Services. There will be no obligation on CAMS to support all the versions of the browser. It shall be user's responsibility for upgrading their/its software, hardware and the operating system at its/their cost from time to time so as to be compatible with that of CAMS. CAMS shall be at liberty to change, vary or upgrade its software, hardware, operating systems, etc., from time to time and shall be under no obligation to support the software, hardware, operating systems used by the user and that the same shall be user's sole responsibility.
5. User / User Entity shall agree that in utilizing the access to the Application, they will conform to the instructions contained in relevant user manual, will follow product licensing norms, and conform to CAMS' Security protocols, as communicated from time to time by CAMS.
6. User / User Entity shall agree that the entity and associated employees shall make no attempts to exceed the privileges provided to the users, and shall make no attempts, directly or indirectly, to reverse engineer, copy or uncompiled the Application.

7. User / User Entity agrees that any of their nominated users shall report any bugs, errors and failures observed in the Application to CAMS on a timely manner with suitable snapshot/logs so that the same may be rectified by CAMS at the earliest.
8. User / User Entity accepts that the Application is a common one intended for use by other users / clients and therefore no features specific to the user can be incorporated into it.
9. User / User Entity agrees to abide by CAMS's Terms and Conditions and rules in force and the changes in Terms and Conditions from time to time relating to the user's account and data access
10. User / User Entity agrees & is / are aware that CAMS will be at liberty to close the user account and / or data access any time without assigning any reason whatsoever.
11. User / User Entity agrees that CAMS may, at its sole discretion, withdraw any of the services/facilities given to user and / or type of access either wholly or partially at any time without giving any prior notice.
12. User / User Entity agrees that any change in user profile information or credentials, using which the user account and / or data access was provided by CAMS to the user, will be immediately informed to CAMS.
13. User / User Entity agrees that all instructions relating to the data access will be issued in writing to CAMS, to CAMS's satisfaction, in form and content.
14. CAMS may offer to open user accounts to selected Customers at its discretion. User / User Entity agrees that in order to be eligible for access to any of CAMS's application, User / User Entity would need to be a legal person capable of entering into a contractual agreement, be a current Internet user or have access to the Internet and knowledge of how the Internet works.
15. User / User Entity accepts that the application for a login access to any of CAMS's software applications / platforms does not automatically imply acceptance by CAMS
16. User / User Entity agrees that User / User Entity shall not use or permit to use electronic or any other access or any related service for any illegal or improper purposes

d) Confidential Information

1. User / User Entity agrees that authorized users who have access to CAMS applications / database / servers shall keep confidential, all information about the Application, hardware, data, the network diagram, the IP addresses, the Network Architecture, the Router Configurations and other technical details that were disclosed and will in future be disclosed by CAMS to the user in order to establish the required connectivity.
2. User / User Entity agrees that the Intellectual Property contained in the Application and underlying database structure belongs to CAMS and User / User Entity shall not dispute the same at any time. No part of the Application, Design, Documentation shared as part of the agreement should be shared or reproduced in any form either fully or partially without written consent from CAMS

e) Anti-Bribery

User / User Entity agrees that User / User Entity shall not pay any amount / consideration in cash or in lieu of cash to any employee of CAMS or any of its associates at the time of securing an access / user account or carrying out any transaction in the normal course of the business. User / User Entity agrees to inform to CAMS's Chief Information Security Officer (CISO) or any other competent authority at CAMS of any person seeking any amount as bribe for provision of such access not authorized by CAMS.

f) Data User Acknowledgment

1. The User / User Entity acknowledges that all information provided in the login account of CAMS application is obtained by CAMS from sources believed by CAMS to be accurate and reliable. Because of the possibility of human and technical error as well as other factors, CAMS is not responsible for any errors of omissions / commissions.
2. The User / User Entity acknowledges that the development of the products and services of CAMS is a continuous process and published information on the Internet may not be up to date.
3. The User / User Entity acknowledges that the formats, update frequency and retention period of the information will be decided at the sole discretion of CAMS.
4. The User / User Entity acknowledges that all information is provided on 'as is' basis without warranty of any kind. CAMS makes no representation and disclaims all

express, implied and statutory warranties of any kind to the user and/or any third-party including warranties as to accuracy, timeliness, completeness, merchantability or fitness of the information for any particular purpose.

5. User / User Entity agrees that CAMS will send suitable communications/letters/alerts, notifications; One Time Passwords etc. through SMS/messenger/mail or through any other mode to the Users at its discretion and CAMS shall not be liable for any loss or delay arising therefrom.
6. User / User Entity agrees that CAMS shall not be liable for any damages, losses (direct or indirect) whatsoever, due to disruption or non-availability of any of services/facility/s due to technical fault/error or any failure in telecommunication network or any error in any software or hardware systems.
7. User / User Entity agrees that CAMS may disclose customer information, in strict confidence, to any of its agent/s and/or contractors with whom CAMS enters or has entered into any outsourcing arrangement in connection with providing of services.

g) Non-Repudiation:

User / User Entity is aware that the transaction through CAMS online platforms, can be affected by use of appropriate PIN or any other similar validations only. User / User Entity shall not request /demand any evidence of proof for transactions undertaken through the online platform/s and the audit trail of the access would be conclusive proof to establish that the transactions are bonafide.

h) Data Protection Guidelines:

To secure the data, users / User Entities that have access to the data or information through our website or mobile devices shall follow the below guidelines which are indicative and not exhaustive.

1. **Always use antivirus software on your personal devices:** Always protect your device with anti-virus software and scan & update it regularly
2. **Keep your operating systems and software up to date:** Have your devices with latest OS and update it regularly
3. **Use Genuine Software:** Always use genuine and updated software to strengthen your online safety and security

4. **Be careful with email attachments:** Do not open the attachments from the unknown source or suspicious email
5. **Application Access Usage:** Use unique user ID and password for usage of any application. No common ID should be used and shared. On need-based access to be provided to the authorized user. The least privilege principle to be followed while providing the access to the users
6. **Data Secrecy:** Always secure confidential data & information
7. **Always keep backup of your data:** Its responsibility of the users to take the data back up and store in secured manner
8. **Data transfer and Storage:** Password controls to be followed while transferring and storing the data
9. **Don't be the source of attack:** The users also should ensure, he/she should not be the source of cyber security attacks
10. **Record the Incident:** If you found any security breach in the data or information, immediately inform to CAMS grievance officer in the below mentioned address
11. **Do not share your privacy:** The sensitive information should not be shared in social media or public domain
12. **Device Safety:** Laptop if any used to be with user ID and password. The laptop should not be kept unattended in public area. Adequate safety measures to be followed while usage in public areas
13. **Removable & Disposal of Media:** Restrict the usage of removable media. If any removable media is used keep in safe custody with password protected. The media should be disposed-off in secured and environment friendly manner. The data stored in devices should be purged periodically in a secured way.
14. **Unauthorized Usage:** Any unauthorized collection, processing or use of CAMS data or information is prohibited. CAMS data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction.

i) Password

User / User Entity understands and agrees:

1. To keep the password totally confidential and not reveal the password to any third party

2. To not use the same password for everything.
3. Use strong passwords of specified lengths as may be prescribed from time to time and which should also include capitals, numbers, and alternate characters which must not relate to any readily accessible personal data such as user's name, address, telephone number, driver license etc. or easily guessable combination of letters and number
4. To commit the password to memory and not record them in a written or electronic form, and not to share / let any unauthorized person have access to computer or leave the computer unattended while accessing CAMS software applications
5. Not provide to any person, at any time, with any details of the accounts held with CAMS including, the passwords, account number, card numbers and PIN (or OTP sent to the registered email id / mobile number) which may be assigned to the authorized user by CAMS from time to time.
6. Not to share the user ID and password to anyone or not to disclose for public view. The user ID & password should not be stored or written down in any soft or in paper form. It is User / User Entity's responsibility to change the password periodically. The users must not use the "Save Password" option in the applications. Other additional controls like Reset password upon first log-in, change of password after 'x' days by default, auto-disabling of password if there is no log-in for 'x' days and so on is also to be implemented
7. In case User / User Entity forgets the login password, User / User Entity can request for change of the password. Such replacement shall not be construed/deemed as the commencement of a new contract.

j) Transaction Processing

1. All the requests for transactions will be given effect to instantaneously to the extent feasible and allowed under the terms of service. In case requests for effecting any transactions are received on weekly offs / holidays / public holidays, they shall be affected on the immediately succeeding working day on the terms and conditions prevailing on that day.
2. User / User Entity shall not hold CAMS responsible for not processing/effecting any transactions in case CAMS does not receive instruction to this effect even though

the User / User Entity may have forwarded the same or if any deficiency is noted at the actual time of transaction processing.

3. User / User Entity have the full right and/or authority to access and avail of the services obtained and the goods purchased / services offered, and User / User Entity shall observe and comply with the applicable laws and regulations in each jurisdiction in applicable territories
4. User / User Entity shall not involve CAMS as a party to such transaction
5. User / User Entity shall provide CAMS with such information and/or assistance as is required by CAMS for the performance of the Services and/or any other obligations of CAMS as envisaged by CAMS, while extending any of these services
6. User / User Entity acknowledges that if any third person obtains access to User's / User Entity's password, such third person would be able to provide/submit Financial Instructions to CAMS on user's / user entity's behalf, at user's / user entity's own risk.

k) Internet Frauds:

1. The Internet per se is susceptible to a number of frauds, misuse, hacking and other actions which could affect data access to CAMS services. Whilst CAMS shall aim to provide security to prevent the same, there cannot be any guarantee from such Internet frauds, hacking and other actions which could affect the services of CAMS
2. User / User Entity shall separately evolve/ evaluate all risks arising out of the same.

l) Mistakes and Errors:

1. The filling in of applicable data for transaction processing or similar such services would require proper, accurate and complete details. For instance, User / User Entity are aware that User / User Entity would be required to fill in the mobile number properly to receive one-time passwords delivered without error. Similarly, in the case of request for redemption, user would be required to fill in the correct details such as the bank account details. In the event of any inaccuracy in this regard, the funds could be transferred to incorrect accounts. User / User Entity shall therefore take all care to ensure that there are no mistakes and errors and that the information given by User / User Entity to CAMS in this regard is error free, accurate, proper and complete at all points of time.

2. User / User Entity agrees that CAMS is providing the Services at User's / User Entity's sole risk.
3. User / User Entity agrees that CAMS shall not be liable for any loss, damages or consequences whatsoever arising due to any erroneous or incomplete information or any delay in executing the instructions for reasons beyond the control of CAMS.
4. On the other hand, in the event of User's / User Entity's bank account receiving an incorrect credit by reason of a mistake committed by some other person, CAMS shall be entitled to initiate efforts to reverse the incorrect credit at any time whatsoever and User / User Entity shall extend all cooperation by giving consent to reverse.
5. User / User Entity shall be liable and responsible to CAMS and accede to accept CAMS's instructions without questions for any unfair or unjust gain obtained by User / User Entity as a result of the same.

m) Technology Risks:

1. The technology for enabling the services offered by CAMS could be affected by virus or other malicious, destructive or corrupting code, programme or macro. It may also be possible that the site of CAMS may require maintenance and during such time it may not be possible to process the request of the Customers. This could result in delays in the processing of instructions or failure in the processing of instructions and other such failures and inability.
2. User / User Entity understands that CAMS disclaims all and any liability, whether direct or indirect, whether arising out of loss of profit or otherwise arising out of any failure or inability by CAMS to honour any customer instruction for whatsoever reason.
3. User / User Entity understands and accepts that CAMS shall not be responsible for any of the aforesaid risks.
4. User / User Entity also acknowledges that, in the event of any such failure, CAMS shall request User / User Entity to resubmit the requests / instructions. Upon written request from CAMS, User / User Entity shall resubmit the instructions.

n) Limits:

1. User / User Entity are aware that CAMS may from time to time impose certain restrictions while accepting requests on its software platform / applications.
2. User / User Entity realize and accept and agrees that the same is to reduce the risks on User / User Entity. For instance, CAMS may impose transaction restrictions within particular periods or amount restrictions within a particular period or even each transaction limits. User / User Entity shall be bound by such limits imposed and shall strictly comply with them.
3. User / User Entity agrees that User's / User Entity's access to the CAMS network shall be limited to browser access to the Application, on an as-is where-is basis, hosted by CAMS, and which application shall be designed to reasonably meet the business requirements of the User / User Entity.

o) Indemnity:

User / User Entity shall indemnify CAMS from and against all losses and damages that may be caused as a consequence of breach of any of the Data Access Terms and Conditions and the terms and conditions mentioned herein above.

p) Binding nature of above terms and conditions:

User / User Entity agrees that by use of any of CAMS services / platforms or applications, User / User Entity shall be deemed to have agreed to all the above terms and conditions and such terms and conditions shall be binding on User / User Entity in the same manner as if User / User Entity have agreed to the same in writing.

q) Authority to CAMS

1. Online transactions in the User's Account(s) are permitted only after authentication of the User-ID and Password. User / User Entity agrees and grants express authority to CAMS for carrying out the online transactions performed by User / User Entity through User / User Entity's login account.
2. CAMS shall have no obligation to verify the authenticity of any transaction received from User / User Entity through User / User Entity's logged in session or purporting to have been sent by User / User Entity via User / User Entity's login account other than by means of verification of User / User Entity's User-Id and the password.

3. The display or printed output that is produced by the user at the time of operation of Online transactions / login account is a record of the operation of the internet access and shall not be construed as CAMS's record of the relative transactions.
4. CAMS's own record of transactions maintained through computer systems or otherwise shall be accepted as conclusive and binding for all purposes unless any discrepancy is pointed out within one week from the date of access or from the date of sending the periodical statement, whichever is earlier.
5. All transactions arising from the use of online services, to operate a joint account, shall be binding on all the joint account holders, jointly and severally.

r) Accuracy of Information

1. User / User Entity agrees that User / User Entity is responsible for the correctness of information supplied to CAMS through the use of User / User Entity's data access or through any other means such as electronic mail or written communication. CAMS accepts no liability for the consequences arising out of erroneous information supplied by User / User Entity.
2. User / User Entity agrees that if User / User Entity notice any error in the account information supplied to them through User / User Entity's logged in access or by the use of any of the online services, User / User Entity shall advise CAMS as soon as possible. CAMS will endeavor to correct the error promptly.
3. All outputs of statements or duplicate statements of account and will be prepared by electronic means and the information contained therein will be extracted from a computerised back up system, maintained at CAMS. While CAMS will take all reasonable steps to ensure the accuracy of the statement, CAMS is not liable for any error. User / User Entity agrees that User / User Entity shall hold CAMS harmless against any loss, damages, etc. that may be incurred/ suffered by User / User Entity, if the information contained in the above said outputs turns out to be inaccurate / incorrect.

s) Liability

1. User / User Entity shall not be liable for any unauthorized transactions occurring through the use of online platforms/applications, which can be attributed to the fraudulent or negligent conduct of the employees of CAMS.

2. If User / User Entity comply with the Terms and advise CAMS in writing under acknowledgment immediately after User / User Entity suspect that User / User Entity's User-Id or password is known to another person and/or notice an unauthorized transaction in User / User Entity's login account / data access, User / User Entity shall not be liable for losses arising out of the unauthorized transactions occurring in the login accounts after the receipt of such advice by CAMS. User / User Entity agrees that User / User Entity shall be liable for some or all loss from unauthorized transactions in the login accounts if User / User Entity have breached the Terms or contributed or caused the loss by negligent actions including the following.
 - a. Keeping a written or electronic record of User-ID and password.
 - b. Disclosing or failing to take all reasonable steps to prevent disclosure of the User-ID and password to anyone including CAMS staff and/or failing to advise CAMS of such disclosure within reasonable time
 - c. Not advising CAMS in a reasonable time about unauthorized access to or erroneous transactions in the login accounts.
3. CAMS shall in no circumstances be held liable to the User / User Entity if data access is not available in the desired manner for reasons including but not limited to natural calamity, floods, fire and other natural disasters, legal restraints, faults in the telecommunication network or Internet or network failure, software or hardware error, cyber-attack or any other reason beyond the control of CAMS.
4. CAMS shall under no circumstances be liable for any damages whatsoever whether such damages are direct, indirect, incidental, consequential and irrespective of whether any claim is based on loss of revenue, investment, production, goodwill, profit, interruption of business or any other loss of any character or nature whatsoever and whether sustained by User / User Entity or any other person.

t) Disclosure of personal information

User / User Entity agrees that CAMS or its contractors may hold and process User / User Entity's Personal Information on computer or otherwise in connection with the services

offered as well as for statistical or such other analysis. User / User Entity also agrees that CAMS may disclose, in strict confidence, to other institutions, such Personal Information as may be reasonably necessary for reasons inclusive of, but not limited to, the following

- For participation in any telecommunication or electronic clearing network
- In compliance with a legal directive
- For fraud prevention purposes.

u) Proprietary Rights

User / User Entity acknowledges the Intellectual Property Rights of CAMS pertaining to Application in the Software Systems, Procedures, Operating, Quality, Control, Audit and User Manuals, Database Design, Screens, Source and Object Code, Reports etc. designed by CAMS and made available to User / User Entity. User / User Entity agrees to keep them confidential, disclose only to employees, auditors or other third-party agents on a need-to-know basis, and not to attempt to reverse engineer or otherwise duplicate these designs directly or indirectly. User / User Entity also agrees that such information will not be disclosed under any circumstances to individuals or entities who / that may have a business interest competitive to that of CAMS.

Access to CAMS's service/s, is a confirmation by User / User Entity that User / User Entity have understood and accepted these terms.

v) Non-Transferability

The grant of facility of CAMS's software-based services to User / User Entity is not transferable under any circumstance and shall be used only User / User Entity.

x) Termination of CAMS's Service/s

1. User / User Entity may request for termination of the online facility / data access provided to User / User Entity any time by giving a written notice of at least 15 days to CAMS. User / User Entity agrees that User / User Entity will remain responsible for any transactions made on User / User Entity's login account(s) through valid access prior to the time of such cancellation of such Service

2. The closure of all User / User Entity's Accounts will automatically terminate CAMS's service/s.
3. CAMS may suspend or terminate data access / online facilities without prior notice if these terms and conditions are breached.

y) Notices

CAMS and User / User Entity may give notices to each other under these Terms and Conditions:

1. Electronically to the mailbox of either party. Such notices will be regarded as being in writing.
2. In writing by delivering them by hand or by sending them by post to the last address given by me/us and in the case of CAMS to the following address:
Computer Age Management Services Limited, Rayala Towers, 158, Anna Salai,
Chennai – 600 002.
3. In case of notice being hand delivered or by post, the same shall be sent to the address last available / updated.
4. In addition, CAMS may also publish notices of general nature, which are applicable to all Customers of CAMS on its web site. Such notices will have the same effect as a notice served individually to me/us.

z) Governing Law & Arbitration

1. User / User Entity agrees that the opening and maintenance of user account is subject to rules and regulations introduced or amended from time to time by the PFRDA, Information Technology Act, 2000 and rules framed there under by Government of India and other applicable laws.
2. These terms and conditions and/or the operations in the accounts of the Customer maintained by CAMS and/or the use of the services provided through any of CAMS's software / online platforms shall be governed by the laws of the Republic of India and no other nation. The Customer and CAMS agrees to submit to the exclusive Jurisdiction of the Courts located in Chennai, India as regards any claims or matters arising under these terms and conditions.
3. CAMS accepts no liability whatsoever, direct or indirect, for non-compliance with the laws of any country other than the Republic of India. The mere fact that the

Services can be accessed through Internet by a Customer in a country other than India shall not be interpreted to imply that the laws of the said country govern these terms and conditions and/or the operations in the login accounts of the Customer and/or the use of online facilities

4. User / User Entity agrees that in case of a dispute, the matter will be settled by arbitration as per the rules of Indian Arbitration and Conciliation Act 1996. Further, the Chief Executive Officer of CAMS or any other person nominated by him will be the sole arbitrator and that the place of arbitration will be Chennai.

aa) Grievance Redressal Mechanism:

Any grievance with respect to data privacy / information security @ CAMS may be addressed to the below mentioned Grievance Officer – Information Security either through email or in writing and such grievance will be redressed within in one month from the date of receipt of the grievance.

Grievance Redressal Officer

Name of the Officer	Address	Email Id
Mr. Kartik S., Chief Grievance Redressal Officer	No. 158, Rayala Towers, Anna Salai, Chennai - 600 002	cracgro@camsonline.com
Mr. Srivatsav K., Grievance Redressal Officer	No. 158, Rayala Towers, Anna Salai, Chennai - 600 002	cragro@camsonline.com

ab) General:

The policy is subject to changes from time to time and the same will be applicable to all users without any obligation on CAMS to communicate the changes. However, this policy will be reviewed at least once in a year or as and when deemed necessary due to requirements of new/change in statues/ regulations/ guidelines/ operating environment.

1. CAMS Data Privacy Policy
2. Employee's Code of Conduct
3. ISMS Standard – ISO/IEC 27001:2013(E)

4. Information Technology Act, 2000 and amendments taking place from time to time
5. Applicable Data Protection Laws
6. PFRDA Circulars / Guidelines issued from time to time in relation to Data protection, Security.