1. Purpose and Scope

This User Management Policy ("Policy") sets out the governance framework, roles and responsibilities, processes, controls and audit-trail requirements for creation, modification, disabling and removal of user access to Elite Wealth Ltd's information systems, databases and applications.
It is designed to ensure that:

- only authorised and appropriately qualified persons ("users") access systems;
- access to applications and databases is based on the principle of least-privilege;
- there is a clear access matrix mapping users, applications and databases;
- audit logs and system controls are in place in line with the NSE circular requirements (including Clause 14 of the circular)
- the definitions of "user", "database" and "application access matrix" are explicitly set out.

The Policy applies to all employees, directors, contractors, third-party vendors (if given access) who are granted user access to Elite Wealth Ltd's systems ("the Firm") whether located onsite, off-site or cloud-based.

---

2. Definitions

For purposes of this Policy, the following definitions apply:

2.1 User
A "User" means an individual (employee, contractor, vendor, consultant) who is assigned a unique system identifier (user ID) that enables them to access the Firm's information systems, applications or databases. The user is an approved person whose access rights are authorised in accordance with this Policy.

2.2 Database
A "Database" means a structured repository of data managed by a database management system (DBMS) or other data-store (on-premises, virtual, cloud) used by the Firm to store client, trading, financial, operational, audit-log or other business-critical information. It includes relational, NoSQL, archive, backup and log-databases relevant to the Firm's operations.

2.3 Application Access Matrix
An "Application Access Matrix" is a documented grid or mapping which identifies for each application (or system module) the roles/privileges, the corresponding databases (or tables) that the application interacts with, the user roles permitted to access each, and the permitted operations (e.g., read, write, delete, execute) for each role. This matrix provides a clear linkage: User Role → Application → Database(s) → Privilege(s).
It is a key control tool for ensuring least-privilege, periodic review of access and alignment with the system audit requirements (for example as per clause 14 of NSE circular)

---

3. Governance and Responsibilities

- **Board / Senior Management** – The Board (or its designated committee) shall approve this Policy and ensure its periodic review (at least annually) and alignment with regulatory / system audit requirements.
- **Chief Information Security Officer (CISO) / Head – IT & Security** – Responsible for implementing and maintaining the user management framework, ensuring compliance with this Policy, maintaining the application access matrix, and liaising with internal/external auditors.
- **IT Operations / System Administrator** – Responsible for executing user account provisioning, modification, disabling/removal, monitoring logs, and maintaining change records.
- **Internal Audit / Compliance** – Responsible for periodic review of user access rights, checking adherence to this Policy, reporting non-compliances to senior management, and coordinating system audits as per the NSE circular.
- **Line Managers / Department Heads** – Responsible for approving user access requests for their teams, ensuring that access is aligned with job-role, removing access when role changes or employment ends.

---

4. User Access Lifecycle

4.1 User Provisioning (Creation)

- A formal access request form shall be submitted (electronically or hard-copy) by the user's department head, specifying: user name, role, justification, applications to be accessed, database(s) if applicable, required privileges.
- The request must be approved by the Line Manager and IT Security (or CISO delegate).
- Based on approved request, IT shall create a unique user ID and assign initial (least) privileges in accordance with the Application Access Matrix.
- A record of the request, approval and provisioning shall be retained.
- Where the access is to a trading, algorithmic, DMA/NNF system (if applicable) the specific regulatory certification requirement must be verified (e.g., for trading members under NSE guidance)

4.2 Modification of Access

- When a user changes job role, location, function or requires additional privileges, a new access-modification request must be submitted, approved, and implemented.
- Privileges removed must also be formally de-approved and implemented in the system.
- The Application Access Matrix shall be updated to reflect the change.

4.3 User Disablement / Removal

- Upon termination of employment, contract, vendor engagement or change of role that no longer requires system access, the user account must be disabled or removed within [for example] 24 hours.
- If the user is inactive (no login) for a defined period (e.g., 90 days) their account shall be disabled pending review.
- All user IDs shall be unique; reuse of user IDs shall be governed by documented policy (e.g., after de-activation and reset period) to avoid audit/log confusion.
- The system auditor must verify that non-compliant users are disabled and audit/event logs are maintained, in accordance with clause 14(d) of the NSE circular.

4.4 Periodic Review / Recertification

- At least annually (or more frequently, e.g., semi-annual for sensitive access) IT Security together with Internal Audit shall review the Application Access Matrix and compare actual user privileges to role-based authorisation.
- Any deviations must be documented, justified and remediated.
- A recertification certificate shall be signed by relevant department head and IT Security stating that user access remains appropriate.

---

5. Access Controls & Privilege Management

- Privileges shall be granted on the principle of **least privilege** – users receive only the access necessary for their role and no more.
- Access to privileged functions (e.g., database writes, system administration, DMA/algorithmic trading) must be restricted to designated roles and require multi-factor authentication (MFA).
- Password policy: unique user IDs, strong passwords, periodic change (e.g., every 90 days), account lock-out on multiple failed attempts, and documented password reset process.
- The firm shall ensure that database segmentation and application segmentation are in place so that only authorised user-roles can access production databases, with separate test/dev environments.
- Data access and change logs must be captured (who logged in, when, what operations performed) and retained in accordance with log retention policy (e.g., minimum 7 years or as per regulatory requirement).
- The Application Access Matrix shall map each application to the databases it accesses and the permitted operations – thereby enabling audits to verify that no user has permissions beyond those mapped.

---

6. Audit, Logging and Monitoring

- All user activity in critical applications (especially trading systems, algorithm modules, DMA, non-front-office systems) shall be logged and monitored.

- The system auditor shall check for adequacy of user management controls (creation/deletion, dormant accounts, access recertification) as required under the NSE circular clause 14.
- Anomalous user behaviour (e.g., login outside business hours, repeated failed login attempts, use of administrator credentials without change record) shall trigger incident review.
- Audit logs shall be protected from tampering (write-once, access-controlled).
- A log-retention schedule must be defined, e.g., event logs retained for minimum 3 years online and archival storage for up to 7 years (or longer if regulatory requirement).
- Reports of user access violations, access recertification exceptions, dormant accounts etc. shall be presented to senior management / audit committee annually or more frequently.

---

7. Application Access Matrix – Maintenance & Usage

- The Application Access Matrix shall be maintained as a live document (electronic) by IT Security, stored in a secure repository, accessible to Internal Audit and the system auditor.
- It shall include fields such as:
    - Application Name
    - Module / Function
    - Database(s) accessed (name, location, production/test)
    - User Role(s) permitted
    - Privilege(s) for each role (Read, Write, Execute, Delete, Admin)
    - Date of last review / recertification
    - Owner (business unit)
- Changes to business processes or application environment must trigger review and update of the matrix.
- During user provisioning or modification the access rights granted shall be cross-checked against the matrix to ensure consistency.
- Internal Audit shall sample check that actual user rights accord with those in the matrix and report exceptions.

---

8. Compliance with NSE/Exchange & Regulatory Requirements

- The firm shall ensure compliance with the requirements of the NSE circular (NSE/INSP/64438 dated 08 Oct 2024) which mandates that system auditors check that the stock broker (trading member) has a well-documented User Management Policy explicitly defining user, database and application access matrix.
- In addition, the firm shall ensure readiness for system audits (Type-III / algorithmic trading, NNF software, etc) and cyber-security audits as required by the Exchange and SEBI.

- The firm shall establish and maintain documentation and evidence of compliance (provisioning logs, approvals, periodic reviews, recertification records) in case of inspection by the Exchange or SEBI.

---

9. Training and Awareness

- All users shall receive mandatory training on information security, user access controls, password hygiene and their responsibilities before being granted access.
- Refresher training shall be conducted annually.
- Specific training shall be provided to privileged users (system-admins, database-admins) on elevated access controls, segregation of duties and monitorisation.

---

10. Segregation of Duties & Termination of Access upon Role Change

- The Policy supports segregation of duties: where feasible no single user should have conflicting privileges (e.g., trading execution + settlement authorisation + system-admin rights).
- When a user's role changes (internal move, promotion, relocation), the old role's privileges must be revoked prior to or at the same time as new privileges are granted.
- Termination of employment or contract shall automatically trigger user access removal in accordance with Section 4.3 above.

---

11. Review of the Policy

- This Policy shall be reviewed at least annually by the CISO in consultation with the Internal Audit/Compliance department, and submitted for approval to the Board (or its designated committee).
- Updates shall be made to reflect changes in business environment, regulatory requirements (including updates from the Exchange/SEBI) and audit findings.

Approved By:

Board of Directors
Elite Wealth Ltd

Last Review Date-25.07.2025
Next Review Due:24.07.2026