
$
30

Terms and Conditions

Regulatory Compliance

The Cipher30 Mentorship is established as a professional educational institution operating from South Africa's financial hub. The Mentorship shall maintain its institutional standing through a rigorous "Logic-Based: educational framework, distinguishing itself from unlicensed financial providers.

1) Institutional Logic v2.4: The Mentorship shall deploy the v2.4 framework, which focuses on price delivery and liquidity. This logic-based approach assumes that "Strategies fail when market conditions change, but Logic adapts," moving students away from static, indicator-based retail strategies.
2) Institutional v2.0 Protocol: All students shall access proprietary education through the secure v2.0 Protocol login system, ensuring the protection of intellectual property (IP).
3) Educational Mandate: The curriculum (Modules 1–4) is specifically engineered to build "Institutional Competence." This serves as a direct response to the competency and operational gaps identified by the Financial Sector Conduct Authority (FSCA) in the broader market.

1.1.2 FSCA Compliance and Boundary Protection

CASP Regulated Activity (FAIS Act)	Cipher30 Operational Reality
Financial Advice: Furnishing "recommendations on... market investment" to a client.	Institutional Competence Training: Teaching the v2.4 logic for reading price delivery. The Mentorship provides rule-based execution models, not specific trade recommendations.
Intermediary Services: Facilitating, managing, or executing trades on behalf of a client.	Rule-Based Education: Students are trained to execute their own trades on proprietary terminals or prop firm challenges (e.g., FTMO/TopOne) based on objective logic, not managed accounts.
Investment Management: The discretionary management of portfolios or crypto assets.	Risk Framework Instruction: Module 3 shall focus on scaling, partials, and drawdown limits to align student-led execution with professional prop firm objectives.

Legal Status of Crypto Assets: The Mentorship defines a "Crypto Asset" as a digital representation of value that applies cryptographic techniques and distributed ledger technology, per FSCA terminology. Adhering to the South African Reserve Bank (SARB) stance, the Mentorship does not recognize crypto assets as legal tender or currency.

FICA and Ethical Conduct

As a relevant entity in the financial education space, Cipher30 maintains an ethical audit trail to mitigate online harms and financial crime.

- FICA RMCP: The business maintains a Risk Management and Compliance Programme (RMCP), documenting an immutable record of transactions to prevent the platform from being utilized for illicit activities.
- Verified Execution: All shared performance data must reflect "Verified Execution" to prevent the dissemination of misinformation or the promotion of fraudulent activities.
- Mandatory Risk Disclosure: Every transaction is governed by a Mandatory Checkout Warning, ensuring students acknowledge that trading involves substantial risk and that the mentorship provides educational content only, not financial services

1.1.3 POPIA Compliance: Data Processing and Accountability

The Mentorship functions as a "Responsible Party" and a Private Body. The following commands shall govern the processing of student data:

- Default Appointment: As Cipher30 is currently headed by a natural person, that individual is the Information Officer by default.
- Authorization: If the founder wishes to designate another individual, they must be at an executive or management level and authorized in writing using Annexure C.
- Registration: The IO must be registered with the Information Regulator before performing any duties. This is a statutory prerequisite under Section 55(2) of POPIA.
- Or if there is no duly regulated or officer available, the person maintaining the website or digital information reliant upon Cipher30 Mentorship is trusted as well as competent in he’s skills and expertise to maintain order, regulation and adherence to the rules and regulations compliant with POPIA and FSCA authorities

8 Conditions for Lawful Processing: Operational Commands

1. Accountability: The Information Officer (IO) shall ensure the POPIA compliance framework is developed, implemented, monitored, and maintained per Section 6.2.1 of the Guidance Note.
2. Processing Limitation: The Mentorship shall only process information required for enrollment (minimality), ensuring consent is obtained for online identifiers and location data.
3. Purpose Specification: Data collected for "Alpha Dispatch" or mentorship access shall not be retained longer than necessary for those specific educational purposes.

4. Further Processing Limitation: Any further use of data must be compatible with the original educational enrollment purpose.
5. Information Quality: The Mentorship shall take reasonable steps to ensure student records are complete and accurate.
6. Openness: The Mentorship shall disclose the specific collection of personal information at the point of initialization.
7. Security Safeguards: Command: Staff shall implement 256-bit encrypted terminal connections and "Zero Spam" policies to prevent unauthorized access or loss.
8. Data Subject Participation: Students retain the right to request access to or correction of their personal information.

Critical Regulatory Warning (Section 57): The Information Officer shall obtain Prior Authorization from the Regulator before processing any unique identifiers (e.g., email/IP) intended to link information with third-party platforms such as Discord or Alpha Dispatch newsletter tools, if such linking is for a purpose other than the original collection.

- Data Footprint: The mentorship does not store extensive personal information. The system primarily utilizes Google Authentication for identity verification and employs one-way encryption (cryptographic hashing) to secure sensitive identifiers, ensuring that personal data is neither retained nor accessible beyond the point of initialization.
- Information Officer (IO): Per Section 55(1) of POPIA, the head of a private body is the Information Officer by default. Currently, the mentorship operates without a separately designated IO; therefore, the founding natural person fulfills all statutory duties of the IO, including the development and maintenance of the compliance framework.
- Condition 7 (Security Safeguards): The mentorship implements 256-bit encrypted connections and "Zero Spam" policies to prevent unauthorized access, loss, or destruction of processed information.

1.1.4 Enrollment Policies (CPA & ECTA)

Enrollment is governed by the Electronic Communications and Transactions Act (ECTA) and the Consumer Protection Act (CPA).

Service Access and IP Policy: The initialization of the "Institutional v2.0 Protocol" constitutes the immediate consumption of proprietary intellectual property (IP). Under ECTA, digital service delivery commences at the point of login generation.

Legal Basis for Non-Refundability:

1. Commencement of Service: Accessing the proprietary v2.4 Logic materials constitutes a rendered service.
2. IP Consumption: The immediate intellectual value provided by the curriculum cannot be "un-consumed" or returned.
3. Access Distinction: The Mentorship provides lifetime access to course materials; however, access to the private Discord community and live sessions depends on the student's active membership plan. This distinction shall be clearly stated to avoid ECTA disputes regarding ongoing service availability.

1.1.5 Strategic Risk Mitigation and Communication

The Mentorship shall actively mitigate both "Online Harms" and "Behavioral Biases" to protect the brand and the student body.

Behavioral Science Integration: Mentors shall utilize Module 4 (Psychology & Discipline) to mitigate specific Behavioral Biases identified by the CFA Institute:

Emotional Biases: Mitigate "Loss Aversion" and "Overconfidence" through the strict application of the v2.4 rule-based execution model.

Cognitive Errors: Counter "Belief Perseverance" by teaching students to adapt to price delivery logic rather than clinging to failing strategies.

Professional Boundary Guide (Discord):

Confidential Thinking Space: Per the Peotona Foundation principle, the Discord community serves as a confidential space for reflection. Mentors shall treat shared student information with care.

Safety and Ethics: In situations where safety or ethical concerns arise, mentors shall refer the participant to the Consultative Support desk for a confidential resolution.

Online Harms: Mentors shall proactively monitor for misinformation and algorithmic bias, ensuring all shared results are "Verified Execution" to prevent financial cybercrime or fraud.

1.1.6 FICA and Anti-Money Laundering (AML)

As a CASP, Cipher30 is classified as an "Educational Institution" under the Financial Intelligence Centre (FIC) Act. The FSCA has planned 30 supervisory inspections for 2025/2026.

Audit Trail Directive: To satisfy a Business Risk Assessment audit, the business must maintain a rigorous Risk Management and Compliance Programme (RMCP). You must document:

1. Institutional Inquiries: A log of all business-level communications.
2. Student Payment Records: An immutable record of all transactions to prevent the platform from being used for obfuscating the source of funds.

1.1.7. Dispute Resolution and Online Harms

Under the Judicial Handbook, "Online Harms" include financial cybercrime and fraud. Refund disputes often escalate into accusations of these harms if not managed through rigorous evidence gathering.

Protocol for Dispute Mitigation

- Mandatory Terms of Service (ToS) Clause: You must implement a clear distinction between "Lifetime Access" (to static course materials) and "Active Membership Plans" (for live community/Discord sessions). Refund disputes for "lack of access" are mitigated if the student retains the core curriculum while losing community privileges.
- Evidence Management: In the event of a dispute, the IO must produce logs of Discord logins and terminal activity. This provides the necessary "Evidence Gathering" to prove service delivery and defend against claims of financial fraud.

1.1.7.a Privacy Policy for EFT and Transactions

To comply with the Protection of Personal Information Act (POPIA), specifically Condition 5 (Information Quality), a responsible party must ensure that personal information is complete, accurate, and not misleading

Mandatory EFT Transference: If payments are processed manually via bank transfer, the Privacy Policy explicitly state: *“Payments are currently processed via EFT/bank transfer. Cipher30 does not store banking passwords, card information, or online banking credentials”*

1.1.9 Checkout Flow Protocol: Immutable Proof of Acceptance

While the framework for "Evidence Management" is established in Section 1.1.8, the following operational protocol must be implemented to provide a complete defence against claims that a student "never saw" or "never agreed" to the terms. The backend of the enrollment system must capture and store an audit trail for every transaction before access is granted:

- Mandatory Checkbox: The enrollment page must feature a mandatory, un-ticked checkbox stating: *“I agree to the Terms, Privacy Policy, and Refund Policy”*.
- Backend Metadata Logging: The system must store the following data points in an immutable log:
    - The IP address of the user at the precise moment they click "I agree".
    - The timestamp (Date and Time) of that agreement.
    - The exact version of the Terms and Conditions that was live at the time of acceptance.
- Audit Readiness: This log serves as your primary evidence during a chargeback dispute or an Information Regulator inquiry to prove that the "Openness" and "Accountability" conditions of POPIA were met.

Cybersecurity and Joint Standard Alignment

While specific Joint Standard 2 of 2024 requirements apply to defined "financial institutions," Cipher30 aligns with these principles to ensure cyber resilience.

- Technological Integrity: Under Section 11 of the FAIS General Code of Conduct, the mentorship maintains appropriate technological systems to eliminate the risk of financial loss through theft or fraud.
- Incident Accountability: The mentorship maintains internal protocols to monitor for material system failures or cyber incidents, ensuring accountability and openness in its digital operations

1.1.10 Mandatory Checkout Warning Text

WARNING: Cipher30 Mentorship is an educational program providing logic-based trade execution frameworks. We do not provide financial advice, signals, or investment management services. By proceeding, you acknowledge that you are responsible for your own trading decisions and that past performance of funded traders is not indicative of future results. ***By purchasing, you confirm that you understand Cipher30 provides educational trading content only and does not provide financial advice or investment services. Due to the digital nature of the mentorship and course access, refunds are generally not available once access has been granted, except where required under South African law. Trading involves substantial risk and results are never guaranteed.***