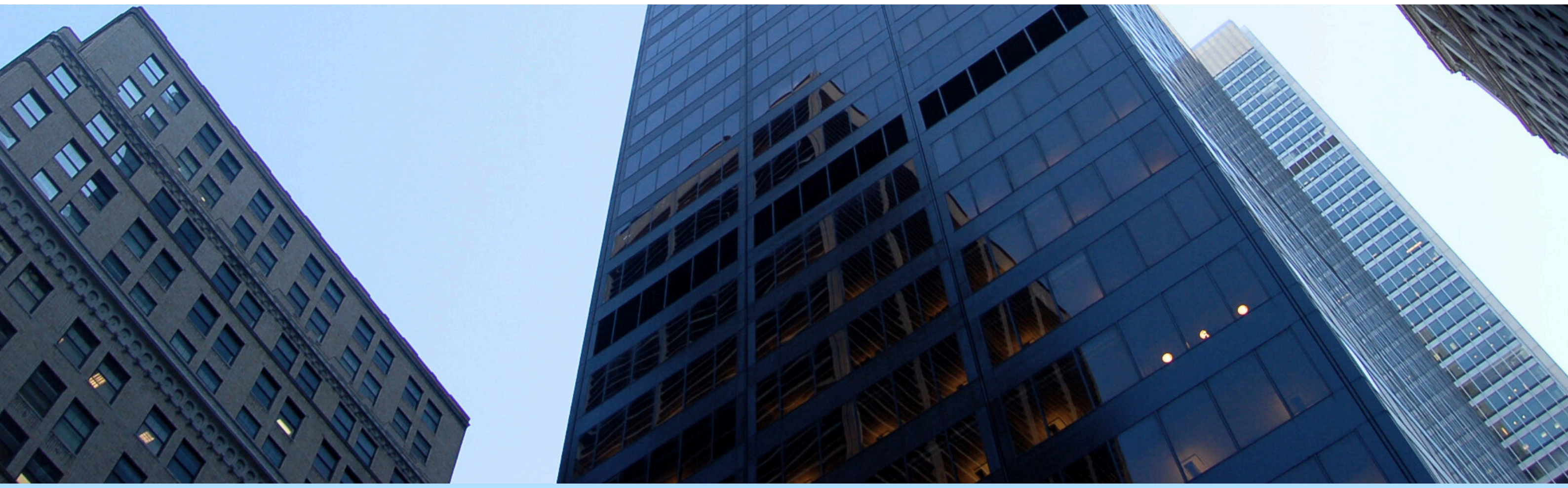
SECURZE

SECURING WHAT MATTERS MOST



SUMMARY OF FIU GUIDELINES 2025

🌐 www.securze.com

✉ info@securze.com

☎ +91 84510 73938

securze

securze_com

securze

INTRODUCTION

On 15th September 2025, the Financial Intelligence Unit of India (FIU-IND) issued updated compliance guidelines for Virtual Digital Asset Service Providers (VDASPs). These guidelines aim to strengthen financial transparency, cyber-security, and anti-money laundering measures in line with India's evolving regulatory framework.

This summary highlights the key requirements in a simplified format for easy reference.

For **registration** or **renewal** with FIU-IND, companies must now submit a Cybersecurity Audit Certificate from a CERT-In empanelled auditor. This certificate is a mandatory part of the documentation required before the in-person meeting.

Documents to be Submitted Before In-Person Meeting:

- **Company Profile**
  - A short note about services offered, and how they fall under the Government's crypto notification (7 March 2023).
  - Ownership and structure details, including an organization chart and identification of Significant Beneficial Owners.

- **Company Records**
  - Registration papers, annual returns, balance sheets, and profit & loss accounts for the last 3 years (as filed with MCA).
  - GST registration certificates for all states where operations are active, plus GST returns for the last 3 years.
  - Income Tax Returns and TDS forms (26Q / 26QF / 26QE) for VDA transactions.

- **Agreements & Partnerships**
  - Copies of agreements with custodians, platforms, brokers, or partners.
  - A short explanatory note on the purpose of each agreement.
  - A PACT certificate (Partner Accreditation for Compliance and Trust) if working with other FIU-registered crypto companies.

- **Declarations & Compliance**
  - A self-declaration confirming no pending cases with ED or other law enforcement agencies.
  - A filled AML/CFT questionnaire (Anti-Money Laundering / Counter Financing of Terrorism).
  - A Cybersecurity Audit Certificate (CERT-In empanelled) confirming compliance with IT Act and CERT-In rules (28 April 2022).

CERT-IN CYBERSECURITY REQUIREMENTS (28 APRIL 2022)

To comply with FIU submissions, the Cybersecurity Audit Certificate must ensure:

- Time Synchronization: Sync all systems with NIC/NPL servers.
- Incident Reporting: Report cybersecurity incidents to CERT-In within 6 hours.
- Technical Point of Contact: Designate an official contact for incident communication (as per CERT-In form).
- Log Retention: Store system logs for 180 days within India.

Data Retention (minimum 5 years): Organizations must store the following details after service withdrawal or cancellation:

- Validated names of customers / subscribers.
- Service usage duration (start and end dates).
- Allocated or used IP addresses.
- Onboarding data: email, IP address, timestamp.
- Purpose for service use.
- Validated address and contact number.
- Ownership patterns of subscribers.

KYC & Transaction Data

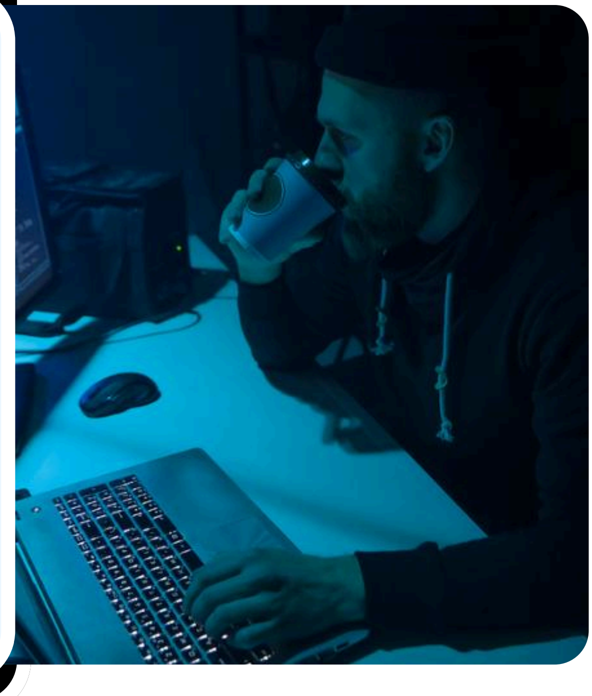
- Retain customer KYC details for 5 years.
- Must include: parties' identification, IPs + timestamps + time zones, transaction IDs, public keys, account addresses, and nature/date/amount of transactions.

REFERENCES

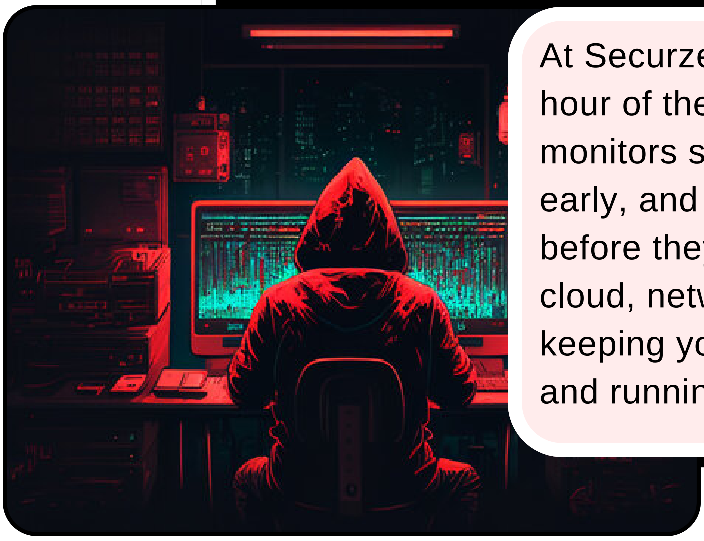
- FIU-IND Guidelines (15 Sept 2025): *Download PDF*↗
- CERT-In Directions (28 Apr 2022): *Download PDF*↗

HOW SECURZE CAN HELP?

At Securze, we simplify end-to-end FIU and CERT-In compliance for Web3 organizations. From conducting CERT-In empanelled cybersecurity audits to building resilient IT and cloud infrastructures, we ensure your business meets every regulatory mandate without disruption. Our expertise spans Web3 Security, VAPT, 24x7 SOC monitoring, incident response, data privacy consulting, and advanced threat simulations. For organisations, this means peace of mind - compliance, security, and business continuity handled by a trusted partner, so you can focus on growth.



24x7x365 MANAGED CYBERSECURITY



At Securze, we protect your business every hour of the day. Our team continuously tests, monitors systems in real time, detects threats early, and responds quickly to stop attacks before they cause harm. We secure your cloud, networks, assets, and applications - keeping your organization safe, compliant, and running without disruption.

Learn More↗

ABOUT SECURZE

Securze (A Cybersecurity Brand Under “Navneetpriya Softech Solutions LLP”) is a global cybersecurity services provider helping organizations achieve end-to-end security and compliance. We specialize in Vulnerability Assessment & Penetration Testing (VAPT), Web3 Security, AI Security, CERT-In empanelled cybersecurity audits, cloud and network security reviews, compliance consulting (DPDPA, ISO 27001, NIST 2.0, GDPR), incident response planning, and attack simulations. Our 24x7x365 Managed Cybersecurity Services provide real-time monitoring, advanced threat detection, and rapid response across IT, cloud, and Web3 ecosystems. With proven experience securing clients across government, Fintech, AI, Web3, Retail, Pharma, Banking, Insurance, E-commerce, Education, Stock Broking, Government, BPO, and many other sectors, we combine technical expertise with business-focused execution to protect operations, ensure compliance, and build long-term resilience.

SECURZE
SECURING WHAT MATTERS MOST

For business inquiries, **contact us.**

www.securze.com	securze
info@securze.com	securze_com
☎ +91 84510 73938	Securze