Member Committee
("MC"/"Committee")
of
National Stock Exchange of India Limited
Exchange Plaza, Bandra-Kurla Complex, Bandra East, Mumbai – 400051
held on May 23, 2025

In the matter of the Trading Member
Angel One Limited

CORAM:

Mr. S Ravindran	-	Chairperson
Justice (Retd.) Ms. Abhilasha Kumari	-	Committee Member
Prof (Dr.) Ms. Mamata Biswal	-	Committee Member
Mr. Essaji Vahanvati	-	Committee Member
Mr. Ashishkumar Chauhan	-	Committee Member

ALSO PRESENT:

Mr. Piyush Chourasia	-	Chief Regulatory Officer
Ms. Sonali Karnik	-	Vice President – Enforcement
Ms. Renu Bhandari	-	Senior Vice President – Inspection
Mr. Janardhan Gujaran	-	Vice President – Enforcement

BACKGROUND

1. **Angel One Limited ("Noticee")** is a Trading Member registered with the National Stock Exchange of India Limited **("Exchange"/"NSEIL")** and enabled for trading in the Capital Market **("CM")** segment since November 1994, Futures & Options ("**F&O**") segment since June 2001, and Currency Derivative ("**CD**") segment since August 2008 and Commodity ("**COM**") segment since February 2021.

2. The Exchange was in receipt of the Immediate Incident Report dated April 24, 2023, from the Noticee, whereby the Noticee reported a cyber security incident ("**Incident**") suspecting a possible data breach having the potential of an external entity gaining access to the Noticee's confidential customer data. The sequence of events is summarized hereunder:

   2.1. On April 20, 2023, the Noticee received an email from angel_one_data@protonmail.com claiming possession of customer data. No sample data was shared in the initial email.

   2.2. Later the same day, the sender provided a cloud storage location containing sample data. Upon review, the Noticee confirmed that the data

was related to its customers. Multiple emails were subsequently received from the same sender with additional data samples.

3. The Noticee submitted a preliminary Root Cause Analysis to the Exchange on April 24, 2023. The RCA identified a vulnerability in a legacy application hosted at trade.angelbroking.com. Several API endpoints and IP hosts (172.31.16.208, 172.31.16.51, 172.31.16.71, 172.31.16.178, 172.31.16.25, and 172.31.16.116) were compromised. The sample data shared by the third party included profile data of 1.32 crore clients and portfolio data of 12.75 lakh records as of August 1, 2021. The sample also included user data up to April 17, 2023.

4. The preliminary Root Cause Analysis (RCA) noted that the vulnerability was linked to the "ClientCode" parameter in the API endpoint /backoffice/AccSummary/DPAccountDetails. The encryption key for this parameter was exposed in the HTML source code. Firewall logs showed high traffic between April 15 and April 18, 2023. The exposed key allowed brute-force attacks to be performed, enabling access to client details without authorization. The schema of the leaked data matched the schema of the legacy API.

5. The Noticee submitted two Root Cause Analysis ("**RCA**") reports certified by a CERT-In empaneled auditor, dated May 10, 2023, and May 25, 2023. The RCA dated May 10, 2023, stated that the incident involved a DDoS attack and installation of malicious files through the user profile of an ex-employee. The RCA dated May 25, 2023, stated that the binary files used by the ex-employee were clean and concluded that the breach was due to vulnerabilities in the legacy API, which allowed brute-force attacks.

6. The RCA dated May 25, 2023, also stated that portfolio data of 12,73,580 clients was breached in August 2021. This indicated that there was no continuous monitoring system in place to detect unauthorized or malicious activities, changes, access, or transmission of data.

7. It is observed that in November 2022, the Exchange had appointed BDO India LLP to conduct a Vulnerability Assessment and Penetration Testing (VAPT) of the Noticee. The assessment was based on a list of critical assets provided by the Noticee, approved by its board in accordance with SEBI circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 7, 2022, and Exchange circular NSE/INSP/52605 dated June 10, 2022. During the assessment, the auditor was unable to access the application trade.angelbroking.com due to non-functional credentials and initiated a black-box assessment. On November 10, 2022, the Noticee informed the auditor that the application was being deprecated and redirected it to trade.angelone.in.

8. The API endpoints linked to trade.angelbroking.com were not included in the list of critical assets and were not covered in the VAPT. Despite instructions from the Exchange on November 1, 2022, to provide a complete list of critical assets, the Noticee submitted incomplete information. Accordingly, a Show Cause Notice (SCN) bearing reference number NSE/INSP/CMFOCDCO/SCN/23-24/Q1/12798/2023-29897 dated July 21, 2023 was issued to the Noticee to seek

an explanation for not submitting the complete list of critical assets, failure to authenticate external facing applications containing sensitive data, failure in deploying adequate controls to address virus/ malware attacks and in establishing monitoring and alert systems for timely detection of malicious activities.

9. In continuation to the SCN, a Supplementary SCN bearing the reference number NSE/INSP/CMFOCDCO/SUPPL-SCN/23-24/Q1/12798/2023-29897, dated January 27, 2025, was issued to the Noticee with additional observations.

INSPECTION OBSERVATIONS/VIOLATIONS

10. The inspection observations/violations alleged in the SCN are summarized hereunder:

10.1. Submission of incomplete details of the critical assets to conduct VAPT assessment.

10.2. Absence of authentication for external facing applications containing sensitive data.

10.3. Failure to establish continuous monitoring systems and processes to facilitate continuous monitoring of security events and failure to analyse traffic patterns and adequate alerts were not kept in place.

10.4. The Noticee failed to deploy adequate controls to address virus / malware / ransomware attacks.

REGULATORY PROVISIONS

11. At the outset, it is appropriate to refer to the relevant regulatory provisions alleged to have been violated by the Noticee; extracts whereof are reproduced below:

11.1. Submission of incomplete details of the critical assets to conduct VAPT assessment

a. Exchange Circular No. NSE/ITRC/40081 dated January 30, 2019 (SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)

Identification

11. Stock Brokers / Depository Participants should identify critical assets based on their sensitivity and criticality for business operations, services and data management…….

12. Stock Brokers / Depository Participants should accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with

the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

Vulnerability Assessment and Penetration Testing (VAPT)

41. *Stock Brokers / Depository Participants should regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.*

41. *Stock Brokers / Depository Participants shall carry out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stock Brokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.*

42. *Stock Brokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stock Brokers / Depository Participants are required to engage only CERT-In empanelled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity.*

In addition, Stock Brokers / Depository Participants shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.

b. Exchange Circular No. NSE/INSP/52605 dated June 10, 2022 (SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022)

11. *Stock Brokers / Depository Participants shall identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system. The Board/Partners/Proprietor of the Stock Brokers / Depository Participants shall approve the list of critical systems.*

To this end, Stock Brokers / Depository Participants shall maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

11.2. <u>Absence of authentication for external facing applications containing sensitive data</u>

a. <u>Exchange Circular No. NSE/ITRC/40081 dated January 30, 2019 (SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)</u>

Protection

<u>Access Controls</u>

15. Stock Brokers / Depository Participants should implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases……

11.3. <u>Failure to establish continuous monitoring systems and processes to facilitate continuous monitoring of security events / alerts and failure to analyse traffic patterns and adequate alerts were not kept in place</u>

a. <u>Exchange Circular No. NSE/ITRC/40081 dated January 30, 2019 (SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)</u>

Monitoring and Detection

45. Stock Brokers / Depository Participants should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.

11.4. <u>The Noticee failed to deploy adequate controls to address virus / malware / ransomware attacks</u>

a. <u>Exchange Circular No. NSE/ITRC/40081 dated January 30, 2019 (SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018)</u>

"*18. Stock Brokers / Depository Participants should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stock Broker / Depository Participant's critical systems. Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc."*

PAST PROCEEDINGS BEFORE MCSGFC

12. The Exchange, vide its email dated March 13, 2024, and April 16, 2024, granted the Noticee an opportunity for a personal hearing before the Committee in its meeting held on April 23, 2024. On behalf of the Noticee, Amit Majumdar- Executive Director, Kush Wadhwa - Senior Director, Pravin Bhathe - Chief Compliance Officer, Bineet Jha Compliance - Officer, Yogesh V Malvankar - CISO, Anupriya Daga - Group Chief Information Security Officer, Pulkit Sukhramani - Counsel, Vidhi Jhawar - Counsel, Deepak Anand – Counsel from Head office of the Exchange at Mumbai and Mr. Jyotiswarup Raiturkar CTO and Chief Architect from regional office of the Exchange attended the personal hearing and reiterated what was submitted by the Noticee.

PRESENT PROCEEDINGS BEFORE MC

13. The matter was again placed before the Committee on May 23, 2025, along with the Supplementary Show Cause Notice issued on January 27, 2025, for the Committee's further deliberation.

CONSIDERATION & FINDINGS

14. After duly considering the oral and written submissions made by the Noticee on the allegations mentioned in the SCN dated July 21, 2023, the Committee observes the following:

14.1. <u>Submission of incomplete details of the critical assets to conduct VAPT assessment</u>

14.1.1. The Exchange observed that the Noticee failed to submit the complete details of the critical assets to conduct VAPT assessment.

14.1.2. In reply to the SCN, the Noticee has submitted as under: -

14.1.2.1. The Noticee has denied the allegation that it submitted incomplete details of critical assets for the VAPT conducted in November 2022. The Noticee explained that it had received an email from the Exchange on August 18, 2022, requesting details of systems/assets/infrastructure components, and in response, it submitted the required information on August 22, 2022. This included the number and types of critical assets, which were later supplemented with a detailed list provided directly to the Auditor. The list covered all critical IT infrastructure, including servers, network devices, security appliances, applications databases, and API collections. The legacy API involved in the cyber incident was part of the TAB application, which was explicitly included in the list of critical assets.

14.1.2.2. The Noticee emphasized that there is no regulatory requirement to provide a separate list of APIs, especially when the parent application has already been disclosed. It further pointed out that the Auditor was able to identify vulnerabilities in APIs integrated within other applications, even without a separate API list, which demonstrates that the information provided was sufficient. The Noticee also clarified that the Auditor conducted a Black Box Assessment, which by design requires the auditor to independently identify vulnerabilities without relying on internal disclosures.

14.1.3. The Committee finds the following: -

14.1.3.1. The Committee notes that the Exchange had communicated to the Noticee via email dated November 01, 2022, and November 04, 2022, to submit a detailed list of critical assets, including a separate sheet for APIs. However, the Noticee failed to provide the required details initially. The Committee finds that the submissions provided by the Noticee to the Exchange subsequently after multiple reminders was incomplete and contained only a summary that mentioned two APIs.

14.1.3.2. Upon verifying the initial list of critical assets submitted on August 22, 2022, the Committee finds inconsistencies with the final list of APIs submitted to the Auditor on October 31, 2022. This discrepancy further raises concerns about the reliability of the Noticee's disclosures and its adherence to the prescribed process for identifying cyber risks and deploying controls, as outlined in Clause 12 of SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, read with SEBI Circular

SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 (the Circular).

14.1.3.3. The Committee finds that the Noticee has failed to provide complete and accurate information regarding its critical assets, as required under Clause 11 of the aforesaid Circular, which mandates Stockbrokers to identify critical assets based on their sensitivity and importance to business operations, services, and data management, and to implement controls accordingly and that all ancillary systems used for accessing/ communicating with critical systems and connections to its network and data flows either for operations or maintenance shall also be classified as critical system.

14.1.3.4. The Committee observes that upon comparison of Noticee's subsequent submission of information on databases and trading API, and the initial submission, the latter lacked the necessary detail and comprehensiveness required under regulatory guidelines. Although the later submission included two APIs and 22 applications (Web/Mobile) along with other technology stack components, it remained insufficient and failed to reflect the complete scope of critical assets at the commencement of the assessment in November 2022.

14.1.3.5. The Committee notes that only on April 26, 2023, the Noticee disclosed the existence of over 2000 APIs in its environment. Thus, the Noticee has failed to maintain and share a comprehensive inventory of critical assets during the initial VAPT request.

14.1.3.6. The Committee observes that despite repeated requests, the Noticee declined to provide login credentials for the "trade.angelbroking.com" application, citing its planned deprecation. As a consequence, the Auditor was constrained to conduct a black-box assessment, which restricted the scope and depth of the testing exercise generally and precluded evaluation of vulnerabilities that would have been discoverable only through authenticated and internal testing. The Committee, however, clarifies that the externally exploitable vulnerability arising from exposure of the encryption key in the HTML source code of the legacy API was, by its very nature, capable of being identified without authenticated access; the non-detection thereof cannot, accordingly, be attributed solely to the absence of credentials, and reflects a wider inadequacy in the VAPT exercise carried out at the relevant time. The lack of authenticated access, taken together with the limited

scope of the assets in fact submitted for assessment, raises serious concerns regarding the adequacy of past assessments and the Noticee's compliance with Clause 41 of the Circular.

14.2. <u>Absence of authentication for external-facing applications containing sensitive data</u>

14.2.1. The Exchange observed that, as per submitted RCA, a legacy API endpoint was found to be unsecure and was identified as the potential source of the user profile data leak by way of matching the schema of the data leaked to the API schema, accordingly it is observed that there is absence of authentication for external -facing applications containing sensitive data

14.2.2. In reply to the SCN, the Noticee has submitted as under: -

14.2.2.1. In response to this charge, the Noticee submitted that it had implemented a comprehensive access policy in accordance with the Cyber Security Circulars issued by SEBI and NSE. This policy governs user access to systems, applications, networks, and databases, and includes strong password controls and multi-factor authentication (MFA). The Noticee clarified that the cyber incident was not due to a complete absence of authentication, but rather due to a specific vulnerability in a legacy API. The API had a parameter called "ClientCode" which was encrypted, but the encryption key was inadvertently exposed in the HTML source code. This unintentional exposure allowed a threat actor to guess the encrypted value and launch brute-force attacks to extract client details.

14.2.2.2. The Noticee emphasized that the field was encrypted and that the exposure was not due to a failure to implement access controls, but rather a coding oversight. The Noticee further stated that all critical systems are protected by robust authentication and authorization mechanisms, and that the compromised API was part of a system that had undergone VAPT. However, the vulnerability was not detected by the Auditor and was instead identified by Noticee's internal Information Security team. The Noticee argued that this demonstrates its proactive monitoring and internal capability, and that the allegation of absence of authentication is misplaced and does not reflect the actual security posture of its systems.

14.2.3. The Committee finds as under: -

14.2.3.1. The Noticee has stated the reason of 'coding oversight' which has led to the issue. The Committee notes that while the Noticee has claimed to have implemented the authentication mechanisms, however, the purported authentication mechanism was present in form but defeated in substance as it was weakened by a coding defect and exposed the encryption key in the HTML source code leading to unauthorized access to its systems. This is evidenced by the data breach involving exposure of the "ClientCode" field, which highlights lapses in access control and the absence of adequate authentication mechanisms for external-facing applications.

14.2.3.2. The Committee observes that the vulnerabilities in the Legacy API went undetected during assessments conducted in 2021–22 which is in violation of Clause 41 of the Circular. The Committee finds that the Noticee itself has admitted to the vulnerability in the Legacy API in its reply and therefore has failed to implement strong encryption and adequate API security on the "trade.angelbroking.com" application. Which subsequently led to the compromise of client codes and exfiltration of sensitive data, which is in violation of Clause 15 of the Circular, which mandates stringent access controls across systems, applications, networks, and databases. Further, the vulnerability in the Legacy API was identified only after the cyber incident, and not during the audit. The non-identification of the said vulnerability during the periodic vulnerability assessment carried out in 2021–22 raises serious concerns regarding the effectiveness and scope of the VAPT processes deployed by the Noticee, and is not in keeping with the requirement under Clause 41 of the Circular, which mandates that periodic Vulnerability Assessment and Penetration Tests be conducted in a manner that enables detection of security vulnerabilities in the IT environment.

14.3. <u>The Noticee failed to establish continuous monitoring systems and processes to facilitate monitoring of security events / alerts and failure to analyse traffic patterns and adequate alerts were not kept in place.</u>

14.3.1. The Exchange observed that as per the audit findings stated in RCA submitted on May 25, 2023, clients portfolio data of 12,73,580 records was breached in August 2021, and that the Noticee has failed to establish continuous monitoring systems and processes to facilitate monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of

data / information held in contractual or fiduciary capacity, by internal and external parties.

The Exchange also observed that adequate mechanisms were not in place to notify alerts about the occurrence of a potential data breach. The failure in the alert mechanism delayed timely detection and mitigation at the data breach.

Further, the Noticee has also failed to conduct a thorough analysis of the traffic pattern during the period from April 15 to April 18, 2023, despite a noticeable spike in database connection indicating abnormal activity. This lapse in monitoring resulted in the failure to identify timely detection of unauthorised or malicious activities.

14.3.2. In reply to the SCN, the Noticee has submitted as under: -

14.3.2.1. The Noticee refuted this allegation by detailing its comprehensive and layered continuous monitoring framework. The Noticee explained that it has implemented systems to detect abnormal network traffic and raise alerts, which enabled its team to identify the data exfiltration activity during the April 2023 incident.

14.3.2.2. The Noticee explained that its infrastructure includes a layered monitoring framework designed to detect and respond to abnormal activity across various components. These systems monitor server-level alerts, endpoint behavior, firewall logs, and volumetric Distributed Denial of Service (DDoS) attacks. The Noticee acknowledged that the portfolio data shared by the attacker was dated August 2021, and during that period, no abnormal traffic patterns were observed—suggesting that the breach may have occurred through low-volume access that did not trigger alerts. However, in April 2023, the monitoring systems successfully detected unusual spikes in database traffic, which prompted immediate remedial action. The Noticee blocked suspicious IP addresses, disabled the vulnerable legacy API, and modified the relevant database procedures to prevent further exploitation.

14.3.2.3. In its submissions, the Noticee also informed the Exchange that it is in the process of transitioning from a manual Security Operations Centre (SOC) to an automated SOC, with implementation targeted by October 30, 2023. The Noticee emphasized that while continuous monitoring systems are designed to detect and mitigate threats, no system can offer absolute protection against all forms of cyber incidents. Nonetheless, the monitoring infrastructure in place proved effective in identifying and containing the

April 2023 breach. The Noticee reiterated its commitment to strengthening its cybersecurity posture through ongoing enhancements to its monitoring capabilities and incident response mechanisms.

14.3.3. The Committee finds as under: -

14.3.3.1. The Committee finds that the Noticee lacked a robust continuous monitoring system, as required under Clause 45 of the Circular. The Circular explicitly mandates real-time monitoring of security events to detect unauthorized access, data transmission, and anomalies across systems exposed to the internet.

14.3.3.2. The Committee observes that the breach involving 12,73,580 client portfolio records went undetected by the monitoring systems. As per the Noticee's response, the systems failed to identify abnormal data traffic, indicating serious gaps in threat detection capabilities.

14.3.3.3. It is recorded, as a matter of factual chronology that the spike in network traffic in the period April 15 to April 18, 2023 was observed by the Noticee only on April 18, 2023, with the Immediate Incident Report to the Exchange being filed on April 24, 2023.

14.3.3.4. The Committee finds that data exfiltration was identified manually by the Noticee's team, rather than through automated alerts. This reflects a failure in implementing effective continuous monitoring.

14.3.3.5. Despite deploying tools, the Noticee did not detect or prevent the breach, raising concerns about the effectiveness of its monitoring infrastructure. The Committee finds that the breach highlights deficiencies in monitoring from 2021 through the incident period. Although the Noticee plans transition to an Automated Security Operations Center by October 30, 2023, no effective system, automated or manual was in place during the breach, which should have detected and mitigated the incident.

14.4. <u>The Noticee failed to deploy adequate controls to address virus / malware / ransomware attacks</u>

The Committee upon deliberation decided that this inspection observation is repetitive and is covered in the inspection observations (mentioned under paragraph 10.2 and 10.3) and that the observation does not warrant separate action.

MEMBER COMMITTEE DECISION

15. In arriving at the quantum of action, the Committee has weighed, by way of aggravation, the scale of the data compromise (profile data of approximately 1.32 crore clients and portfolio data of approximately 12.73 lakh records), the duration over which the initial compromise remained undetected (from in or about August 2021 until April 2023), and the nature of the Noticee's obligations as a Trading Member holding sensitive client data in a fiduciary capacity, and, by way of mitigation, the immediate remedial steps taken by the Noticee upon detection (including blocking of suspicious IP addresses, disabling of the legacy API and modification of the relevant database procedures), the subsequent transition from a manual to an automated Security Operations Centre, the identification and disclosure of the vulnerability by the Noticee's internal information security team, the Noticee's cooperation through the course of the inspection and these proceedings, and the absence of any material on record evidencing pecuniary loss to the affected clients arising from the Incident.

Having regard to the above, the Committee is of the view that the appropriate course is to record a warning, together with the directions set out below, rather than to impose any further sanction.

In view of the above, the Committee decided to Warn the Noticee for the observed violations and directed the Noticee the following:

a. To put in place systems and processes to monitor and analyze the traffic pattern on a continuous basis to detect spikes in database connection.
b. To ensure continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information.
c. To ensure adequate control on the maintenance of API Inventory including ownership, criticality/impact of APIs and secure usage of all APIs as outlined in Exchange circular dated NSE/INSP/62912 dated July 11, 2024.
d. To provide confirmation on the implementation of above-mentioned controls by CERT-IN empaneled auditor within 45 days from the date of communication.
e. The Noticee is advised to ensure compliance with all the requirements of the SEBI Circular no. SEBI/HO/ ITD-

1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024, on 'Cyber Security and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)' enclosed with the NSE Ref. NSE/INSP/63502 dated August 21, 2024 and subsequent circulars, clarifications and FAQs relating to Cyber Security issued from time to time.

Abhilasha Kumari
(Committee Member)

Essaji Vahanvati
(Committee Member)

Ashishkumar Chauhan
(Committee Member)

Date: May 29, 2026