Website: www.cbose.com

CENTRAL BOARD OF OPEN SCHOOLING AND EXAMINATION

"Serving under the national framework for open schooling and vocational education, in alignment with the guiding principles of the National Education Policy (NEP) – Government of India."

C-77 Cluster Place, Peeragarhi- New Delhi 110001
Ph: 9557361231, 9557351231

Ref No: CBOSE/EAM/2025/307 **Date: - 15 March 2025**

Press Release

Digital Result Authentication & National Academic Document Security Policy – 2025

It is hereby notified for the information of all affiliated study centres, regional digital compliance units, district-level IT monitoring cells, institutional heads, examination superintendents, ABC integration officers, verification authorities, cybersecurity officers, and all stakeholders functioning under the Central Board of Open Schooling & Examination (CBOSE), that in alignment with the Ministry of Education, Government of India, and in accordance with the Digital India Academic Stack, DigiLocker Governance Protocol, National Credit Framework (NCrF–2025), and the National Academic Integrity Initiative, the Board is implementing the **Digital Result Authentication & Academic Document Security Policy – 2025**.

This Notification supersedes all previous instructions issued regarding digital document security, result verification, certificate authentication, migration record issuance, and protection of academic credentials from misuse, duplication, forgery, or unauthorized alteration. This policy has been formulated to ensure the highest standards of academic security, national verification uniformity, and international credibility of credentials issued by the Board.

The Ministry of Education has emphasized that institutions must transition completely from conventional paper-based documentation to a secure digital academic environment with QR authentication, blockchain-backed verification, encrypted digital signatures, tamper-proof result pages, and AI-based anomaly detection systems. Accordingly, all academic documents issued by CBOSE during and after 2025 shall be **digitally sealed, real-time verifiable, tamper-proof, and stored in the National Academic Depository and DigiLocker ecosystem**.

From the academic year 2025 onwards, **no physical document shall be treated as authentic unless supported by digital authentication**. The Board clarifies that printed marksheets, physical passing certificates, laminated copies, and institution-issued manual duplicates shall not carry legal validity unless they contain digitally verifiable QR codes linked directly to the Board's verification server.

Institutions must ensure that every learner obtains a DigiLocker account linked with Aadhaar or an approved digital identification token. It shall be the responsibility of institutional digital compliance officers to guide learners in activating their DigiLocker Academic Wallet and ensure smooth integration with the Academic Bank of Credits (ABC). No student shall be allowed to download or access certificates until their ABC ID and digital identity have been authenticated.

All results shall be published **exclusively** on the digital examination portal. Learners must log in using their secure credentials. After the release of the digital result, the Board shall

automatically generate **Digital Mark Sheets**, **Digital Migration Certificates**, **Digital Provisional Certificates**, and **Digital Passing Certificates**, each embedded with encrypted QR codes, blockchain identifiers, digital signatures, and certificate tracking numbers. These documents shall automatically sync with the learner's DigiLocker and ABC Wallet.

The QR code printed on each academic document shall redirect the verifier to a secure link containing encrypted metadata, including learner details, document issuance date, document authenticity code, verification timestamp, and certification status. Any modification, manipulation, screenshot editing, or alteration of the document shall be detected by the system instantly.

Institutions must instruct learners to never submit non-QR documents to universities, employers, government bodies, or international agencies. External bodies including embassies, universities, recruitment boards, and credential evaluators must be directed to verify the authenticity of documents using the **National Academic Verification Portal**, where the Board shall provide real-time confirmation of document status.

The Board warns institutions that unauthorized printing, stamping, photocopying, or distribution of any academic document without digital verification constitutes academic malpractice. Centres must not create their own provisional result sheets, marksheets, centre-generated transcripts, or printed duplicates. Only the digitally sealed documents issued by the Board carry official validity.

Institutions must maintain secure handling of all digital records. Every centre must have a designated Digital Security Officer. This officer must ensure that no unauthorized device, public-access computer, or unsecured Wi-Fi network is used for result downloads or certificate handling. Centres must maintain a log of all digital downloads conducted on their premises for audit purposes.

The Board also mandates implementation of **AI-based Anomaly Monitoring**, which will detect suspicious login activity, irregular result download patterns, unauthorized mass generation attempts, or document manipulation indicators. Centres found involved directly or indirectly in creating, supporting, or facilitating fraudulent practices shall face strict administrative action including suspension of affiliation, withdrawal of examination rights, or legal proceedings under relevant laws.

All academic documents must be stored digitally by institutions for internal archival. Hard copies must not be retained unless required temporarily for verification. The Board shall conduct periodic audits to ensure compliance with digital record-keeping protocols.

Learners with disabilities or limited digital access shall be provided guided support at their centres. Institutions must ensure that such learners are not denied access due to technological constraints. Centres must maintain a digital assistance desk equipped with a counselor or trained IT representative.

The Board instructs all institutions to adopt **multi-factor authentication** for administrators handling examination-related data. Password sharing is strictly prohibited. All administrative accounts must use biometric or OTP-based authentication. Centres must maintain an incident log for any suspicious digital activity.

In case of discrepancy in digital records, learners must apply through the official **Digital Grievance Window**. Physical applications shall not be accepted. All corrections must be made strictly based on verified demographic documents authenticated earlier during the Pre-Result Verification Cycle.

Institutions must ensure that communication regarding digital verification is transparent. Institutions may not issue handwritten notes or local certificates confirming student results. Any such attempt will be deemed misconduct.

The Ministry of Education has mandated national uniformity in academic documentation. Therefore, all institutions must clearly communicate to learners that **only digitally issued documents carry national and global recognition**. The Board shall not respond to verification requests submitted outside the Digital Verification Portal.

This Notification must be displayed prominently on all institutional boards, digital screens, learner notice areas, and official communication groups. Heads of institutions must ensure strict adherence to this Notification by all departments.

This Notification supersedes all previous instructions issued by CBOSE regarding digital result, certificate authentication, and document verification.

This issues with the approval of the Competent Authority.

Copy with a request to respective Heads of Directorates as indicated below to also disseminate the information to all concerned schools under their jurisdiction:

1. All Regional Directors/Regional Officers of CBOSE with the request to send this circular to all the Heads of the affiliated schools of the Board in their respective regions
2. All Joint Directors/Deputy Directors/Assistant Directors, CBOSE
3. In charge IT Unit with the request to put this circular on the CBOSE websites
4. The Assistant Librarian, CBOSE
5. The Public Relations Officer, CBOSE
6. PS to Chairperson, CBOSE
7. SPS to Secretary, CBOSE
8. Guard File

CENTRAL BOARD OF OPEN SCHOOLING & EXAMINATION
Organization Secretary
CBOSE
॥ नास्ति विद्यासमं चक्षुः ॥

Organization Secretary

Central Board of Open Schooling and Examination, New Delhi