Proctored Exam Data Storage Policy

1. Purpose

This policy outlines the guidelines for storing data related to proctored exams for a minimum of five years, ensuring data security, privacy, and compliance with relevant regulations.

2. Scope

This policy applies to all employees, contractors, and third-party service providers involved in the administration, proctoring, and management of exams.

3. Types of Data Collected

- Exam Records: Student information, exam details, scores, and timestamps.
- Proctoring Data: Audio, video recordings, and screen captures.
- Incident Reports: Logs of any irregularities or issues during the exam.

4. Data Security

- Encryption: All data must be encrypted in transit and at rest using industry-standard encryption protocols.
- Access Control: Access to exam data should be restricted to authorized personnel only, with role-based access controls implemented.
- Authentication: Multi-factor authentication (MFA) should be required for accessing the data storage systems.

5. Data Privacy

- Consent: Ensure that students are informed about the data collection and storage practices and obtain their explicit consent before the exam.
- Anonymization: Where possible, anonymize data to protect the privacy of the students.

6. Data Retention

- Retention Period: All proctored exam data must be retained for a minimum of five years from the date of the exam.
- Review and Purge: After the retention period, data should be reviewed and securely purged unless required for ongoing legal or compliance reasons.

7. Data Access

- Access Logs: Maintain detailed logs of who accessed the data, when, and for what purpose.
- Audit: Regular audits should be conducted to ensure compliance with this policy.

8. Data Disposal

- Secure Deletion: Data should be securely deleted using methods that prevent recovery.
- Documentation: Maintain records of data disposal activities, including the method used and the date of disposal.

9. Compliance and Legal Requirements

- Regulatory Compliance: Ensure the data storage practices comply with relevant local and international regulations (e.g., GDPR, CCPA).
- Legal Holds: In the event of legal proceedings, place a hold on data deletion and inform relevant stakeholders.

10. Policy Review and Updates

This policy should be reviewed annually and updated as necessary to ensure it remains relevant and effective.

11. Responsibility

- Data Protection Officer (DPO): Responsible for overseeing the implementation and compliance with this policy.
- IT Department: Ensures technical measures for data security and storage are in place.
- Proctoring Team: Ensures compliance with data collection and retention practices.

By implementing this policy, we can ensure the secure and compliant storage of proctored exam data for the required period while respecting the privacy and rights of the students.