DATA GOVERNANCE POLICY

THE SUPERIOR UNIVERSITY LAHORE

SUPERIOR UNIVERSITY

DATA GOVERNANCE POLICY

(Applicable to Learning Management System (LMS) and Content Management System (CMS))

I. Scope

This Data Governance Policy applies comprehensively to all institutional data generated, processed, transmitted, archived, or stored through Superior University's Learning Management System (LMS) and Content Management System (CMS). The scope of this policy extends to all faculty members, students, administrative staff, IT personnel, academic leadership, contractual employees, consultants, third-party service providers, and any external affiliates who are granted access to institutional digital systems.

The policy governs data irrespective of its format (digital, cloud-hosted, archived, backup, exported reports) and irrespective of the hosting model (on-premises servers or managed cloud infrastructure). It encompasses academic data, administrative data, authentication credentials, activity logs, course materials, assessment records, analytics outputs, and publicly displayed CMS content.

This policy shall remain binding regardless of the location from which systems are accessed, including remote or international access environments.

II. Policy Statement

Superior University recognizes that institutional data is a strategic academic and operational asset that directly impacts educational integrity, institutional credibility, regulatory compliance, and stakeholder trust. The University is committed to establishing a robust governance framework that ensures data confidentiality, integrity, availability, accountability, and lawful usage throughout its lifecycle.

The objective of this policy is to create a structured and sustainable data governance environment that ensures responsible digital conduct, accurate academic record management, transparent assessment practices, controlled system access, and systematic protection against misuse, unauthorized disclosure, or cyber threats.

Through this policy, the University affirms its commitment to safeguarding academic records, protecting student information, preserving intellectual property, and maintaining high standards of digital accountability.

III. Governance Structure and Oversight

A. Data Owner (Director Information Technology)

The Director Information Technology shall serve as the institutional Data Owner and primary Data Trustee for all LMS and CMS systems. In this capacity, the Director IT bears ultimate responsibility for ensuring that technical infrastructure, storage environments, system architecture, and cybersecurity controls meet institutional standards and regulatory expectations.

The Data Owner shall:

- Establish and approve data governance standards and security protocols.
- Ensure implementation of encryption, authentication, backup, and disaster recovery mechanisms.
- Oversee classification frameworks and access control structures.
- Report data risks, vulnerabilities, and compliance status to senior leadership.
- Ensure that LMS and CMS platforms align with national and international cybersecurity benchmarks.

The Director IT shall also coordinate with academic leadership to ensure that technical controls support academic integrity requirements.

B. Academic Data Steward (Director ODL – LMS)

The Director Open & Distance Learning shall act as Academic Data Steward for all academic and assessment-related data stored within the LMS. The Academic Data Steward holds responsibility for ensuring that the academic use of digital systems maintains transparency, fairness, traceability, and alignment with University policies and regulatory frameworks.

Responsibilities include:

- Oversight of digital assessment integrity and grade accuracy.
- Monitoring regular testing compliance and audit readiness.
- Ensuring that LMS data reflects approved academic structures.
- Coordinating with QA units for compliance audits.
- Reviewing anomalies in assessment logs or grade changes.

The Academic Data Steward ensures that academic data governance complements technical security controls.

C. Data Custodian (IT Department)

The IT Department shall function as Data Custodian and is responsible for day-to-day operational management of LMS and CMS systems. This includes implementing security controls, maintaining server health, performing routine backups, monitoring access logs, applying patches and updates, and safeguarding infrastructure against cyber threats.

The IT Department must ensure continuous monitoring mechanisms are in place to detect unauthorized access attempts, abnormal activity patterns, or potential vulnerabilities.

D. Authorized Users

All members of the University community who access LMS or CMS platforms are responsible for using institutional data strictly within the scope of their academic or administrative role. Users shall not extract, replicate, manipulate, or distribute institutional data beyond authorized purposes.

All users are required to complete mandatory data security awareness training and acknowledge their responsibility in maintaining digital integrity.

IV. Data Classification Framework

To ensure appropriate protection levels, all LMS and CMS data shall be formally classified into one of four categories. Classification determines the level of security, access restriction, and handling requirements.

Level 1 – Restricted (Highest Sensitivity)

This category includes highly sensitive institutional data that, if improperly accessed or disclosed, could result in severe institutional, legal, or reputational harm.

Examples include:

- Student grades and transcripts
- Examination attempts and activity logs
- Personally identifiable information (PII)
- Authentication credentials
- Financial and payment-related records

Such data must be encrypted during storage and transmission, accessible only to authorized personnel with role-based approval, and continuously monitored through audit logs.

Level 2 – Sensitive

This category includes institutional data that may not be legally restricted but requires careful management to prevent institutional risk.

Examples include:

- Question banks
- Faculty evaluation records
- Internal performance analytics
- Operational planning reports

Sensitive data must be stored within secure University environments, with controlled access permissions and encryption strongly recommended.

Level 3 – Internal

This includes proprietary institutional data intended solely for internal operational use.

Examples include:

- Course outlines
- Internal announcements
- Administrative workflow documents

Access shall be limited to authorized University members and may not be publicly disseminated without formal approval.

Level 4 – Public

This includes institutional information approved for public access, such as CMS-hosted program descriptions or official announcements.

Public data does not require encryption but must maintain accuracy and authenticity.

Any data not explicitly classified shall default to Level 1 (Restricted) until formally categorized.

V. Data Handling and Protection Standards

All classified data shall be handled in accordance with established institutional standards.

Access Control

The University shall enforce role-based access control (RBAC), ensuring users only access information required for their defined responsibilities. Access privileges shall be reviewed periodically and revoked immediately upon termination or role change.

Data Transmission

All restricted and sensitive data transmitted electronically must utilize secure encrypted channels such as HTTPS or secure file transfer protocols. Email transmission of restricted data must employ encryption safeguards.

Data Storage

Restricted and sensitive data must be stored exclusively on University-approved servers or compliant cloud infrastructure. Storage environments must adhere to security benchmarks defined by the IT Directorate.

Backup and Disaster Recovery

The University shall implement automated daily backups, secure off-site storage, and periodic restoration testing to ensure resilience against data loss. Disaster recovery plans shall prioritize academic continuity and minimal disruption.

VI. Data Integrity and Audit Mechanisms

All system interactions involving academic data must be traceable. Grade changes, assessment modifications, or administrative overrides must leave permanent system logs. Manual alteration of logs is strictly prohibited.

Audit logs shall be retained for a minimum of two years, while academic records shall be retained for at least five years. Periodic joint audits by IT and QA departments shall ensure system transparency and reliability.

VII. Data Breach Management

Any suspected or confirmed data breach must be reported immediately to the Director IT. Incident response protocols shall include investigation, containment, impact assessment, leadership notification, and corrective measures.

Failure to report breaches or negligent handling of institutional data may result in disciplinary action.

VIII. Data Retention and Archival Standards

(Aligned with HEC Regulatory and Quality Assurance Expectations)

Superior University shall retain and archive institutional LMS and CMS data in strict accordance with Higher Education Commission (HEC) guidelines, institutional academic regulations, statutory requirements, and recognized digital record-keeping standards applicable to higher education institutions.

Data retention practices shall ensure academic traceability, regulatory audit readiness, student record protection, and institutional continuity.

a. Academic Record Retention

All academic records generated through the LMS—including but not limited to:

- Student grades and gradebooks
- Quiz and examination attempts
- Assignment submissions
- Assessment rubrics and evaluation feedback
- Activity completion reports
- Attendance and participation records

shall be retained for a minimum period of **five (5) years** from the date of course completion, or longer where required by HEC, accreditation bodies, legal obligations, or University statutes.

For ODL and blended learning programs, digital assessment evidence shall remain retrievable to demonstrate compliance with HEC academic monitoring and quality assurance requirements.

b. Examination and Assessment Logs

System-generated logs relating to:

- Quiz attempt timestamps
- Submission records
- Grade modification history
- Access and authentication logs
- IP-based activity records (where enabled)

shall be retained for a minimum period of **two (2) years**, or longer if required for audit investigations, academic appeals, disciplinary reviews, or accreditation inspections.

These logs shall remain tamper-resistant and auditable.

c. Data Archival Controls

Archived LMS and CMS data shall:

- Be stored in secure University-controlled environments
- Maintain the same confidentiality classification as active data
- Be protected against unauthorized alteration or deletion
- Remain encrypted where classified as Restricted or Sensitive

Access to archived data shall require formal authorization from the Director IT or designated Data Steward and shall be documented for audit purposes.

d. Backup and Preservation Integrity

In alignment with HEC's emphasis on digital evidence preservation for academic transparency, the University shall:

- Perform automated daily backups of LMS and CMS databases
- Maintain secure off-site backup copies
- Conduct periodic restoration testing to ensure data recoverability
- Document backup procedures and retention schedules

Backup integrity reports shall be maintained for compliance verification.

e. Regulatory and Audit Compliance

Retention schedules shall support:

- HEC Quality Enhancement Cell (QEC) audits
- Academic Council reviews
- Program accreditation inspections
- External evaluation visits
- Student grievance or appeal investigations

Archived records must remain retrievable in a readable format capable of demonstrating academic authenticity and institutional due diligence.

f. Secure Disposal

Upon expiration of the defined retention period, data disposal shall be conducted in a secure and irreversible manner, ensuring that Restricted or Sensitive data cannot be reconstructed.

Disposal processes shall be documented and approved by the Data Owner.

g. Exceptional Retention

Data may be retained beyond the standard schedule in cases involving:

- Ongoing litigation
- Regulatory investigation
- Academic misconduct inquiries
- Accreditation review processes

Such extensions shall be formally documented.

IX. Compliance and Enforcement

Adherence to this policy is mandatory. Non-compliance, misuse of institutional data, unauthorized disclosure, or violation of access controls may result in disciplinary measures, suspension of system privileges, or legal action where applicable.

X. Review and Continuous Improvement

This policy shall undergo review every three years or sooner if necessitated by regulatory changes, technological upgrades, or institutional restructuring. Amendments require approval from competent authority.

If you would like, I can now:

- Expand this into a Board-ready formal document
- Add an ISO-aligned cybersecurity annexure
- Add a Risk Assessment & Control Matrix
- Add an HEC ODL compliance mapping table
- Create a one-page executive approval summary

Let me know your intended approval forum.

VIII. Data Retention and Archival Standards Institutional data shall be retained in accordance with defined retention schedules. Archived data remains subject to confidentiality protections and shall be accessible only through controlled authorization procedures. enhance the point as per HEC standard

Certainly. Below is an **enhanced and HEC-aligned version** of Section VIII – Data Retention and Archival Standards, written with stronger regulatory positioning, audit defensibility, and academic compliance framing suitable for Higher Education Commission (HEC) expectations, particularly in ODL and digital academic environments.

Data Governance Policy

"Data Governance Policy" provides a comprehensive framework for safeguarding institutional data across all formats and access points, ensuring confidentiality, integrity, and accountability. It details the roles and responsibilities of faculty, staff, and IT personnel in managing sensitive information while adhering to regulatory standards. Through stringent access controls, data classification, and retention practices, this policy affirms the University's commitment to protecting academic records and maintaining digital security in a rapidly evolving technological landscape.