Sample: Data Governance Plan for NeoTech University

In an era where data is a critical asset, NeoTech University recognizes the importance of a structured and secure data governance framework. They have established the policies, procedures, and best practices required to ensure institutes' data integrity, security, and management. It fosters a responsible data culture, enabling informed decision-making and safeguarding the university's data assets for the future.

Let's look at the data governance plan that will help you to complete the **Lab: Create Data Governance Plan for FutureMart**.

Section 1: Define the purpose and scope

Purpose of the data governance plan The data governance plan at NeoTech University ensures that data is accurately managed, protected, and used to support institutional decision-making, enhance student experience, and comply with regulatory standards. The plan focuses on promoting transparency, security, and accountability in how data is handled and utilized across the university.
Scope This plan covers all data used and generated by the university, including student records, faculty and staff data, academic performance, financial data, research data, and administrative records. It applies to all departments and systems, including the learning management system (LMS), student information system (SIS), and human resources software.

Section 2: Data governance objectives

Data quality Ensure that data used across all departments is accurate, complete, and up to date to support decision-making, academic outcomes, and operational efficiency.
Data security

Safeguard sensitive data such as student records, financial information, and health data against unauthorized access and data breaches.

Data compliance

Comply with applicable laws and regulations, including Family Educational Rights and Privacy Act (FERPA), General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA).

Data availability

Ensure that critical data is accessible to authorized users across the university, facilitating operations and academic excellence.

Data usage

Use data effectively to improve student outcomes, optimize university operations, and support strategic planning, while respecting privacy and ethical standards.

Section 3: Data governance framework

Roles and responsibilities of data governance team members

Data governance steering committee

The steering committee oversees the implementation and monitoring of the data governance plan.

Members:

- **President (Dr. Sarah Johnson):** Committee Chair
- **Chief Information Officer (CIO, Mark Williams):** Technology Oversight
- **Chief Financial Officer (CFO, Emma Miller):** Financial Data Oversight
- **Vice President of Academic Affairs (Dr. John Black):** Academic Data Oversight
- **Director of Compliance (Grace Lewis):** Compliance and Privacy Oversight
- **Chief Data Officer (CDO, Michael Lee):** Data Stewardship and Quality Oversight

Data stewards

Data stewards are responsible for ensuring that the quality, integrity, and usage of data within their departments adhere to governance standards.

Roles:

- **Student data steward (Nancy Peterson):** Responsible for managing students' records, grades, and academic performance data.
- **Faculty data steward (Dr. Linda Adams):** Responsible for handling professors' records, academic qualifications, and teaching data.
- **Financial data steward (Robert Chang):** Responsible for managing financial records, including tuition payments, grants, and donations.
- **Research data steward (Dr. Mark Lee):** Responsible for managing research data, publications, and academic research records.

Data owners

Data owners make decisions regarding how data is used and shared.

Roles:

- **Registrar's Office (Thomas Wright):** Owner of students' academic records and transcripts.
- **Human Resources (Sandra Brown):** Owner of employee and faculty data.
- **Finance Department (Clara Fisher):** Owner of financial and accounting data.

Data users

Data users include university staff, faculty, and administrators who need access to data for operational purposes.

Roles:

- **Admissions Team** – Uses student data to process applications and admissions.
- **Academic Advisors** – Accesses student academic records to guide students in course selection and degree progress.

Section 4: Data management best practices

Data classification

Data classification of university data into categories to ensure appropriate data management:

- **Public**: Information meant for public consumption, such as course catalogs, and public research publications
- **Internal**: Non-sensitive data used for internal operations (e.g., faculty schedules, internal communications)
- **Confidential**: Sensitive data requiring protection (e.g., student academic records, financial information, faculty contracts)
- **Restricted**: Highly sensitive data requiring the highest level of protection (e.g., medical records, research data with privacy considerations)

Data quality management

- Implement data validation rules in all data entry points to reduce errors and inconsistencies.
- Create regular audits for data quality, focusing on completeness, accuracy, and timeliness of data.
- Establish data cleansing processes for removing outdated or duplicate data from university systems.

Data integration

Ensure that all university systems, for example, SIS, LMS, HR software, and financial systems, are integrated to maintain a consistent flow of data across departments, minimizing data silos, and ensuring data is accurate across platforms.

Data documentation

Maintain a data dictionary that includes metadata, data definitions, and usage guidelines for all university data. Update the dictionary regularly to ensure its accuracy and relevance.

Section 5: Data security and privacy policy

Data encryption and masking

- Encrypt all sensitive data, including student financial and medical information, in storage and during transmission.
- Mask sensitive data where possible, for example, only showing the last four digits of a student's social security number (SSN) or credit card number in reports.

Data access control

- Implement role-based access control (RBAC) across all systems to ensure that employees, faculty, and students only access the data necessary for their roles.
- Use multifactor authentication (MFA) for systems storing sensitive data, such as the SIS or financial records.

Incident management

- Develop a formal process for responding to data security breaches, including immediate reporting protocols, investigation procedures, and communication plans.
- Affected individuals will be notified within 48 hours of any breach involving their personal information.

Section 6: Data compliance and legal consideration

Regulatory requirements

- **FERPA**: This law ensures the privacy of students' education records and gives them the right to access and request corrections to their records.
- **GDPR**: Comply with EU students' data protection rights when processing their personal data.
- **HIPAA**: Protect student health information, especially when students use health services at the university.

Data audit and reporting

- Conduct annual data governance audits to assess compliance with regulations and internal policies.
- Submit regular reports to the data governance steering committee and promptly address any compliance failures.

Data retention and disposal

- Develop a data retention policy that ensures compliance with legal requirements and university policies. For example, data retention of academic records for a specific period after graduation.
- Securely deleting or archiving data that is no longer needed according to defined retention schedules.

Section 7: Data governance tools and technologies

Data management systems

- **Student information system (SIS)**: Leverage Ellucian Banner for managing student data, course registration, and grades
- **Learning management system (LMS)**: Use Blackboard for managing course content, grades, and assessments.
- **Financial management system**: Use Workday for managing payroll, tuition, and donations

Data governance software

- **Collibra**: Used for managing metadata, data quality, and compliance workflows.
- **Informatica**: Leverage for data integration and data quality monitoring.

Data monitoring and reporting tools

- **Tableau**: Used for data visualization and reporting on academic performance, student engagement, and financial health.
- **Power BI**: For internal performance metrics, including faculty performance, departmental budgets, and operational efficiency.

Section 8: Data governance training and awareness

Training programs

- Conduct mandatory training for new employees, faculty, and staff on data governance policies, data security, and privacy regulations.
- Offer annual refresher courses for all university staff and faculty to stay current on data governance best practices.

Ongoing awareness campaigns

- Update monthly newsletters for the university community on data governance news, including best practices, policy changes, and data security tips.

Section 9: Performance metrics and reporting

Key performance indicators (KPIs)

- **Data quality**: Record the percentage of accurate and complete student records and missing data across departments.
- **Security compliance**: Record the number of data breaches and the time to respond to incidents.
- **Regulatory compliance**: Record the percentage of compliance with FERPA, GDPR, and HIPAA.
- **Operational efficiency**: Note time taken for data access requests and response times for data issues.

Reporting structure

- Provide monthly reports to the data governance steering committee, covering KPIs and incidents.
- Share quarterly updates with the university's leadership team.

Section 10: Implementation plan

Timeline

- **Phase 1 (0-3 months)**: Establish the data governance steering committee, define roles, and implement data quality checks.
- **Phase 2 (4-6 months)**: Roll out access control mechanisms, implement data integration, and begin the first data audit.
- **Phase 3 (6-12 months)**: Launch training programs, refine compliance processes, and assess the effectiveness of the data governance tools.

Resources and budget

- Allocate approximately $250,000 for the first year, focusing on training, software licenses, and hiring two data governance specialists.
- Dedicate 3 FTEs to manage data governance operations.

Summary

NeoTech University's data governance plan is important for managing the increasing volume of data while ensuring its accuracy, security, and compliance with legal standards. Implementing robust data governance best practices supports NeoTech University's academic mission, enhances students' experience, and ensures responsible and efficient use of data across the University.