**NAME-ANKUSH KUMAR**

**ROLL NO.-16006**

**DATA PRIVACY**

**CLASS-B.SC.(HONS) CS SECTION-A**

**Data Privacy Audit Report**

Organization: Keshav Mahavidyalaya (Delhi University)

Audit Date: October 25, 2024

Auditor: Ankush Kumar

Objective: Assess data privacy practices to identify vulnerabilities and ensure compliance with relevant data protection regulations.

1. **Scope Definition**

Objective: Assess the collection, processing, and storage of student, staff, and faculty data to identify privacy risks and ensure compliance with applicable regulations (e.g., GDPR, CCPA).

Scope: Includes student and staff databases, admission systems, online student portals, and departmental databases involved in data handling.

Limitations: Excludes data managed solely by third-party vendors.

1. **Data Types and Sources Identification**

Data Types:

- Personal Data: Names, contact details, ID numbers, academic records, health data.

- Sensitive Data: Health and disability information, financial data (scholarships, fees).

-Financial Data: Payment history, bank account details for payroll and reimbursements.

Data Sources:

- Internal: Registration forms, academic records, payroll systems.

- External: Online admission portal, third-party assessment tools.

Data Flow Mapping :

- Collection: Data is collected via online admission forms, departmental requests, and academic portals.

- Processing: Data is processed for admissions, academic record-keeping, and financial disbursements.

- Storage: Data is stored in central and departmental databases with restricted access.

- Sharing: Data is occasionally shared with third parties (e.g., scholarship bodies, exam boards) with explicit agreements.

1. **Policies and Procedures Review**

Privacy Policy Review:

Keshav Mahavidyalaya's privacy policy was reviewed for compliance with GDPR, as the university enrolls international students.

Finding:

The policy adequately addresses data collection and user rights but lacks clarity on third party data sharing.

Data Retention Policy:

Data retention periods vary by data type. Student records are kept indefinitely, while financial data is retained for 7 years. Finding: Retention policy aligns with industry practices but could benefit from more granular guidelines on sensitive data retention.

Incident Response Plan:

The university has a documented response plan with designated response teams. Finding: The plan is comprehensive but lacks a formal testing schedule to ensure readiness.

1. **Compliance Assessment**

Regulatory Compliance:

GDPR compliance verified, as international data transfers occur for student records. Local privacy laws (India's IT Act) are also adhered to. Finding: Generally compliant, but improvements are recommended for clearer privacy notices during data collection.

Internal Standards

Finding: University follows ISO 27001 guidelines but does not have formal certification.

1. **Data Inventory and Classification**

Data Inventory:

All data types were listed, detailing personal, sensitive, and financial data held by each department.

Data Classification:

Data has been classified as public, internal, and sensitive, with appropriate access controls in place.

Finding:

Classification and access levels are well-defined but should be updated annually.

1. **Access Controls Review**

User Access: Access is role-based, with sensitive data limited to authorized personnel.

Finding: Access levels are appropriate but could be refined with stricter criteria for sensitive data access.

Authentication Methods: Multi-factor authentication (MFA) is implemented for all sensitive systems. Finding: Strong authentication controls; regular audits of MFA effectiveness are recommended.

1. **Security Measures Assessment**

Data Encryption: Data is encrypted in transit using HTTPS protocols; sensitive data at rest is also encrypted.

Finding: Encryption is robust; however, an upgrade to end-to-end encryption for all data is suggested.

Network Security: Firewall and intrusion detection systems are in place. Finding: Network security measures are effective; annual penetration testing would further strengthen security.

Physical Security: Data servers are located in secure, monitored facilities.

Finding: Physical security is sufficient; monthly access reviews for server rooms are advised.

**8.Third-Party Risk Assessment**

Vendor Management:

Contracts with third-party vendors include data protection clauses.

Finding: Vendor agreements are thorough but could benefit from annual compliance checks.

Data Sharing Agreements:

Data sharing agreements with scholarship boards and exam bodies are well-documented. Finding: Review frequency should be increased to ensure compliance with evolving privacy regulations.

1. **Training and Awareness**

Employee Training: Data privacy training sessions are conducted annually.

Finding: Training is effective but lacks specific content on handling sensitive data.

Awareness Campaigns: Monthly email reminders and posters are used to promote data privacy best practices. Finding; Awareness initiatives are consistent; including interactive workshops could improve engagement.

1. **Incident History Review**

Breach History: A minor data breach occurred in 2022 due to a phishing attempt.

Finding: Incident was well-managed, but phishing resistance could be improved through additional training

Mitigation Measures: Post-breach measures include improved email filtering and staff training.

Finding: Measures are effective; expanding phishing simulations could further strengthen defense.

1. **Risk Assessment and Reporting**

Identified Vulnerabilities:

Potential risk of over-access due to broad access control.

Minor risk with third-party data sharing compliance.

Risk Prioritization: High priority for access control refinement. Medium priority for third-party compliance monitoring.

Report Findings: Summary of findings, prioritized recommendations, and action plan were documented and shared with university management.

1. **Follow-Up and Continuous Improvement**

Regular Audits: Annual audits are scheduled to maintain data privacy standards.

Feedback Mechanism: A feedback loop was established to incorporate suggestions and maintain continuous improvement.

Conclusion: Keshav Mahavidyalaya is largely compliant with data privacy standards, although some areas for improvement have been identified, including enhanced access controls, third-party compliance checks, and more frequent incident testing. Recommendations were provided, and a follow-up audit is scheduled for the next year.