TU Data Privacy Act Overview and Data Removal Requirements

1. Overview of the Data Privacy Act

The term **'Data Privacy Act'** in the United States most commonly refers to the **Privacy Act of 1974**. This federal law governs how U.S. federal agencies collect, maintain, use and disclose personal information. Although Tuskegee University is not a federal agency, the principles of the Privacy Act strongly influence higher education privacy practices and are reflected in FERPA, GLBA, HIPAA and NIST standards.

2. Core Principles of the Data Privacy Act

The Privacy Act of 1974 establishes foundational privacy principles, including notice of data collection, purpose limitation, access and amendment rights, safeguards to protect data, retention limits and accountability.

3. Applicability to Tuskegee University

While Tuskegee University is not directly subject to the Privacy Act of 1974, similar obligations arise through FERPA for student records, GLBA for financial data, HIPAA for health-related records, state privacy laws and NIST Privacy and Security Frameworks.

4. Definition of Data Removal

Data removal refers to the authorized and secure elimination of data from systems, devices, backups, media and third-party platforms when the data is no longer required for institutional, legal, or regulatory purposes.

5. Types of Data Removal

Data removal methods include deletion (logical removal), destruction (physical or cryptographic wiping), anonymization, de-identification and archival expiration.

6. Data Removal Requirements

All data removal activities must be authorized by the designated Data Owner, aligned with records retention schedules, performed using secure NIST-aligned methods, logged for audit purposes and suspended when legal holds apply.

7. Third-Party and Vendor Data Removal

Vendors and service providers must contractually agree to securely remove TU data upon request or contract termination and provide written certification of data deletion, including removal from backups.

8. Data Subject Requests

Where permitted by law, individuals may request correction or removal of personal data. Requests shall be reviewed in coordination with Legal Counsel and Records Management.

9. Restrictions on Data Removal

Data must not be removed if required by FERPA retention rules, audit requirements, grant conditions, financial regulations, or legal holds.

10. Governance and Oversight

Data removal activities fall under the oversight of the Data Privacy Officer, CIO, CISO, Legal Counsel and Records Management in accordance with the University Governance Charter.