ADMINISTRATIVE PROCEDURE

ITP-TBD

DATA PRIVACY POLICY

Number: ITP-TBD	Name: DATA PRIVACY POLICY
Purpose: Marshall University is committed to safeguarding the privacy of individuals and the confidentiality of institutional data. This procedure outlines the minimum privacy and security requirements for all technology systems that collect, store, process, or transmit personal or institutional data. It supports the university's broader information security objectives as defined in the Information Security Policy (UPGA-10) and aligns with applicable federal and state regulations, including FERPA, HIPAA, and GLBA.	

Responsible Unit: Information Technology	
Approved by:	Approval Date:

1. General
   This procedure applies to all faculty, staff, students, contractors, and third-party agents who use or manage technology systems that manage institutional data. It encompasses all data types and systems, whether hosted on-premises or in the cloud, and includes both university-owned and vendor-managed platforms. It complements the Technology Governance and Procurement Review Procedure (ITP-1), which governs the acquisition and oversight of technology systems. The definitions of key terms in this policy are defined in the UPGA-10 Information Security Policy.

2. Data Classification and Handling Procedures

   2.1 General
   Institutional data must be classified according to its sensitivity and risk level, as outlined in the university's data classification guidelines referenced in UPGA-10. Data is categorized as Restricted, Confidential, or Public. Restricted data includes personally identifiable information (PII), financial records, health data (PHI), and student academic records (FERPA). Confidential data includes internal communications, research data, and personnel evaluations. Public data includes information intended for public dissemination, such as course catalogs and press releases. Each classification level requires specific handling procedures to ensure appropriate protection throughout the data lifecycle.

2.2 Technical Safeguards

Technology systems that store or process Restricted data must implement encryption at rest and in transit, role-based access controls, and multi-factor authentication. They must also retain comprehensive logging with a minimum six months retention period. Systems managing Confidential data must encrypt data in transit and are strongly encouraged to encrypt data at rest. Access controls and logging are required, with logs retained for at least six months. Public data systems may operate with fewer restrictions but must still follow university-approved security practices. These safeguards should be consistent with the expectations outlined in federal and state regulations, ITP-1, and UPGA-10. Marshall University Information Technology (MUIT) maintains an inventory of all systems and types of data processed. For systems not owned and/or maintained by MUIT, an administrator of the system must be identified and shall be responsible for ensuring adherence to this policy.

2.3 Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (PIA) is required for any new or significantly modified system that processes Restricted or Confidential data. The PIA is documented during the Technology Request Review process, as outlined in ITP-1. The PIA must identify the types of data collected, assess potential privacy risks, and document mitigation strategies. The assessment must be reviewed and approved by the university's Chief Information Officer (or designee) and the Information Security Office prior to system deployment. This requirement supports the university's commitment to proactive risk management and transparency in data collection.

2.4 Vendor and Cloud Service Requirements

All third-party vendors that process institutional data must enter into a Data Processing Agreement (DPA) with the university. Vendors managing Restricted data must demonstrate compliance with relevant data protection standards, such as FERPA, HIPAA, or SOC 2. MUIT will conduct annual reviews of vendor compliance and data handling practices. The review requirement can be met using standardized security assessment questionnaires such as the HECVAT (Higher Education Community Vendor Assessment Toolkit). These expectations are consistent with the procurement and oversight responsibilities outlined in ITP-1, Technology Governance and Procurement Review.

2.5 User Responsibilities

All users of university systems are responsible for protecting the privacy and security of institutional data. Users must complete annual privacy and security training. Each department must designate a Data Steward responsible for ensuring compliance with this procedure. Any suspected or confirmed unauthorized access, disclosure, or loss of institutional data must be reported to the Information Security Office within 24 hours of discovery, in accordance with the incident response procedure defined in UPGA-10.

2.6 Privacy Protections

Privacy protections for individuals with data stored in Marshall University systems are outlined on the Marshall University website at the following location: https://www.marshall.edu/privacy-policy/ and https://www.marshall.edu/privacy-policy/gdpr/.

2.7 Review and Maintenance

This procedure will be reviewed annually by the Information Security Office, Chief Information Officer, and Chief Data Officer. Updates will be made necessary to reflect changes in technology, regulatory requirements, or university operations. Non-compliance with this procedure may result in disciplinary action and/or revocation of access to university systems.