Data Policy

Revised September 17, 2024

I. SCOPE

This policy applies to all academic and operational departments and offices at all Tennessee Wesleyan University locations, owned and leased. The policies and procedures provided herein apply to all University faculty, staff, students, visitors, and contractors. This policy governs the privacy, security, and confidentiality of university data, especially highly sensitive data, and outlines the responsibilities of institutional units and individuals for such data.

II. POLICY STATEMENT

Tennessee Wesleyan University maintains data essential to the performance of university business. These data are valuable assets. State and federal laws identify the types of data to which access and storage must be restricted. This policy incorporates federal and state standards and establishes responsibilities for all elements of university data in terms of confidentiality, integrity, and availability.

The greatest benefit the university can provide to the community is data that is shared and used with care. This benefit is diminished through misuse, misinterpretation, or unnecessary restrictions on access. Although a large portion of university data are shared with the public, some data are restricted by the privacy protections established in laws or policies. To comply with these mandates and to protect the university community, the university has the right and the obligation to protect, manage, secure, and control data under its purview.

III. DEFINITIONS

A. University Data

University data are any data required to conduct the operations of the university. University data are divided into two main categories: protected data and public

use data. Protected data include two subcategories: highly sensitive and restricted.

- **Protected Data – Highly Sensitive:** Data that (1) by their personal nature can lead to identity theft or exposure of personal health information, or (2) a researcher, funding agency, or other research partner has identified as highly sensitive or otherwise requiring a high level of security protection. Some examples are: data classified as secret by the Federal government, data that is often involved in identity theft (e.g., SSNs), data described in the Health Insurance Portability and Accountability Act (HIPAA) as needing to be secured, and data that could lead to financial theft (e.g., credit card information).

- **Protected Data – Restricted:** Data that by their very nature or regulation, are private or confidential and must not be disclosed except to a previously defined set of authorized users. Some examples are: data defined as confidential by the Family Educational Rights and Privacy Act (FERPA), employee performance evaluations, confidential donor information, some research data, minutes from confidential meetings, accusations of misconduct, or any other information that has been identified by the University, its contractors or funding agencies, or Federal or State regulations, as private or confidential and not to be disclosed.

- **Public Use Data:** Data intended for public use. An example is the university's online directory.

- **Encryption:** Encryption is the conversion of data into a form that is unreadable by an unauthorized user or process. Encrypted data must be decrypted (converted back to the original form) prior to use. The university's centrally managed encryption method requires a key for encryption and decryption. Data Custodians must employ encryption as a means of protecting Highly Sensitive Data.

B. **Key Personnel Responsible for the Protection of University Data**

- **President:** The president of Tennessee Wesleyan University has ultimate responsibility for the university's security program and the protection of restricted and highly sensitive data and critical system assets. The president has delegated these responsibilities to members of the president's cabinet and senior leadership team.

- **Chief Information Officer (CIO):** The university officer designated by the university president to have executive oversight of the university's IT security program and for the evaluation and classification of data.

- **Chief Data Stewards:**

    - **Vice President for Financial Affairs:** The cabinet member designated by the university president to be responsible for all highly sensitive and restricted data associated with donors, employees, contractors, students, and affiliates. In this role, the Vice President for Financial Affairs determines who has access to such data, how it can be stored, and how it must be protected. The Vice President for Financial Affairs may delegate responsibility for certain data sets to others.

    - **Vice President for Academic Affairs:** The cabinet member designated by the university president to be responsible for all restricted and highly sensitive data associated with students and faculty in performance of their teaching and research activities. In this role, the VPAA determines who has access to such data, how it can be stored, and how it must be protected. The VPAA may delegate responsibility for certain data sets to others.

    - **Vice President for Institutional Effectiveness and Research: :**The cabinet member designated by the university president to be responsible for all data associated with institutional effectiveness, research, and reporting for same. In this role, the VPIER determines who has access to such data, how it can be stored, and how it must be protected. The VPIER may delegate responsibility for certain data sets to others.

- **Information Security Officer (ISO):** An individual designated by university leadership or whose role may be served by the Chief Information Officer (CIO) to be responsible for the development, implementation, oversight, and maintenance of the university's IT security program, or the person designated as the University's Qualified Individual (**QI**) for the purposes of compliance to the Gramm-Leach-Bliley Act (**GLBA**) Safeguards Rule.

- **Data Owners:** Deans, vice presidents, associate vice presidents, directors, managers, or others authorized by the Data Governance Committee (see below) to manage a subset of data.

- **System Administrator:** A System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the University, Data Owner, and/or Data Custodian. Their responsibilities can include administration at the

system infrastructure layer and/or system application layer. Any given system may have more than one System Administrator depending on the size and complexity of the system. The System Administrator assists with the day-to-day administration of the university's IT systems and implements security controls and other requirements of the IT security program on IT systems for which the System Administrator has been assigned responsibility.

- **Data Custodians:** An individual who has been authorized to be in physical or logical possession of data by the Data Owner.

- **Data Processors:** An individual authorized by data owners to enter, modify, or delete data.

- **IT System Users:** Any university employee, contractor, affiliate, or duly authorized member of the community who can access restricted and/or highly sensitive university data but does not modify or delete that data. For the purposes of the responsibilities section in this policy, IT System Users include all who have the capacity to access university data. All IT System Users, whether they be Data Owners, Data Custodians, or Data Processors, are responsible for the security and privacy of the data they access, as prescribed in this policy.

- **Customer:** Any employee, student, or individual not associated with the university from whom highly sensitive data are collected or received.

- **University Data Committees:** Any committee charged by the university to create and enforce data protections, decision making, risk assessments, or remediations in the service of providing persistent governance under the direction of some of all the Chief Data Stewards of the university.

IV. RESPONSIBILITIES

A. General

Access to university data is provided to university employees for the conduct of university business. Protected data, as defined by this policy, will be made available to employees who have a genuine need for it. This may include data collected from students, faculty, staff, contractors, members of the community, or those who have no affiliation with the university. Employees accessing such data must observe the requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data used in any type of reporting function. Individual units or departments that have stewardship responsibility for portions of

protected university data must establish internal controls to ensure that university policies are enforced. All IT System Users, not just Data Owners, Data Custodians, or Data Processors, are responsible for the security and privacy of the data they access or store, as prescribed in this policy.

B. Compliance

The university forbids the disclosure of protected data in any medium except as approved in advance by a Data Owner. The use of any protected university data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity is strictly prohibited. Each IT System User will be responsible for the consequence of any misuse of university data. The university forbids the storage of highly sensitive data on any data storage device or media other than a centrally managed server approved for the storage of highly sensitive data, services explicitly approved for the purpose and specific data classification through the Data Governance Committee, or a secure networked file storage area. If an individual is required to store highly sensitive data for a business need, that individual must obtain permission from the Chief Information Officer or designated Qualified Individual (QI). The written request for authorization must state the unique business need, the type of data that will be stored, the type of data storage device that will be used, and the mitigating controls that will be employed to protect the highly sensitive data.

Any university employee, student, or non-university individual who stores highly sensitive university data without proper permissions and protection measures is in violation of this policy and will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.

Should a security breach occur, the chief information officer will confer with University Leadership and the University's Legal Counsel as to whether the matter should be referred to law enforcement and those with insurable interests in the university. The Director of Human Resources will review all matters involving university employees. The Vice President of Student Affairs will review all matters involving students. University Legal Counsel will review matters involving individuals not affiliated with the university.

All individuals accessing university data at Tennessee Wesleyan University are required to comply with federal and state laws and university policies and procedures regarding data security of highly sensitive data. Any university employee, student, or non-university individual with access to university data who engages in unauthorized use, disclosure, alteration, or destruction of data is in violation of this policy and will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.

C. **The Duties of Key Personnel**

Authorization for access to and the maintenance and security of all university data, particularly highly sensitive data, is delegated to specific individuals within their respective areas of responsibility.

- **Chief Data Stewards Responsibilities:**
    - Establish policies and direction for the overall security and privacy of all University data, particularly highly sensitive data, within their respective areas of responsibility.
    - Identify and appoint Data Owners for units within their areas of responsibility.
    - Designate personnel to review privacy and compliance inquiries and respond or escalate them appropriately.

- **System Owner Responsibilities:**
    - Require that all users of the system complete required IT security awareness and training activities prior to, or as soon as practicable after receiving access to the system, and no less than annually, thereafter.
    - Manage system risk and develop any additional IT security procedures required to protect the system in a manner commensurate with risk.
    - Maintain compliance with university IT security policies and standards in all IT system activities.
    - Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.
    - Designate a System Administrator for the system. See System Administrator Resources – Information Technology Services for a list of System Administrator resources.

- **Data Owners Responsibilities:**
    - Ensure that access and protection requirements consistent with university policies and the data classification are in place and responsive to business needs.
    - Ensure the accuracy and quality of all data within their area.
    - Communicate data protection requirements to the System Owner.
    - Annually review with appropriate Data Custodians the current set of highly sensitive data access authorizations and, as appropriate, update authority granted each user.

- Ensure that authorized users of highly sensitive data are trained on their responsibilities associated with their approved access to that data.
- Report any possible breach in computer security or illicit use of highly sensitive data to the Support Center who will then notify the Chief Information Officer.
- Review appeals to decisions denying access to university data within their area of responsibility.

- **System Administrators Responsibilities:**

  - Identify possible security gaps that may leave systems vulnerable to attacks or hacking and take remedial actions to secure the systems.
  - Ensure the usability, reliability, availability, and integrity of information systems and their data, including serving as liaisons between all parties with interests in such systems.
  - Follow established formal procedures and tools as determined by their respective Data Owner to enable access for authorized Data Processors and IT System Users. This includes ensuring that all specified approvals have been granted before providing an IT System User access to highly sensitive data.
  - Maintain documentation of users who are authorized access to highly sensitive data on IT systems to which they have been assigned. Where abuses of that authorization are discovered, make authorization withdrawal recommendations to the appropriate Data Owner.

- **Data Custodian Responsibilities:**

  - Protect the data in their possession from unauthorized access, alteration, destruction, or usage.
  - Use IT systems in a manner consistent with university policies and procedures. A Data Custodian may also be a System Administrator.

- **Data Processors Responsibilities:**

  - Responsible and accountable for the completeness, accuracy, and timeliness of the data assigned to them.
  - Ensure the accurate input and presentation of data. Each Data Processor will be responsible for any intentional misrepresentation of data.

- Ensure the maintenance of data integrity. Upon recognizing that any data elements are in error, the Data Processor will notify the appropriate Data Owner.

- **IT System Users Responsibilities:**

  - Use restricted and highly sensitive data only as required by the employee's job responsibilities and authorized by the appropriate Data Custodian.
  - Respect and protect the confidentiality and privacy of individuals whose records they access.
  - Report any possible breach in computer security or illicit use of restricted and/or highly sensitive data to the Data Owner of the IT System User's unit.

D. **Organizational and Individual Responsibilities for Access Control to Highly Sensitive Data**

No one is permitted to access highly sensitive data unless warranted as part of an established job role. The user must not store the data unless written approval has been granted to do so using the online form that requires the user to describe the unique business need for storage and the mitigating security controls.
Each department or business unit will have documented procedures, consistent with the university's security policies, which preserve and protect highly sensitive data and are designed to accomplish these goals:

1. Ensure the security and confidentiality of customer information.
2. Protect against any anticipated threats to the security or integrity of such information.
3. Guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Each Data Owner will have a documented set of procedures for reviewing requests to access, modify, or update highly sensitive data.

The IT Department will be available to assist each department or business unit by reviewing their access and data security procedures. If needed, the privacy and compliance personnel will review to ensure compliance with this policy.

Members of the university community may appeal any decision that denies access to university data. Appeals are to be made to the appropriate Data Owner.

E. **Public Requests for Protected Data**

Requests by the public for protected data made through the Tennessee Public Records Act or other applicable law will be reviewed by the University's Legal Counsel prior to any release of data.

V. TRAINING

Managers are responsible to train, or arrange for training, for all current employees who have or will have access to highly sensitive university data prior to granting access to such data.

VI. Exclusions and Omissions

Data oversight and responsibilities not expressly described within this policy are governed by the established technology and IT acceptable use policies of the university, or by the appropriate university data governance committee.