

MIDDLE TENNESSEE STATE UNIVERSITY
POLICIES AND PROCEDURES MANUAL

POLICY NO.: I:03:06

DATE: July 1, 2009

SUPERSEDES POLICY NO.: I:03:06

DATED: September 25, 2008

SUBJECT: Information Security Policy

APPROVED: Sidney A. McPhee, President



I. Purpose

The purpose of this policy is to ensure the confidentiality and integrity of MTSU's information assets. This policy pertains to all University information assets, whether the assets are individually or departmentally controlled; enterprise managed; stand-alone; and/or stored via electronic, paper, or other media. The policy reflects MTSU's commitment to stewardship of sensitive personal information and critical business information, in acknowledgement of the many threats to information security and the importance of protecting the privacy of University constituents, safeguarding vital business information, and fulfilling legal obligations. It is MTSU's intent to protect the personal information of its students, staff, faculty, alumni, and other individuals associated with the University from unauthorized access or disclosure, and possible misuse or abuse.

This policy is designed to establish awareness and provide guidance on the proper handling of personally identifiable information (PII) including individual social security numbers (SSN) maintained by or on behalf of MTSU. PII is defined in Section IV of this policy. MTSU has implemented this policy to reduce the risk of exposure when PII is used as a primary identifier at the University and in other valid business applications and ensure that all PII is handled consistently throughout the University. Personally identifiable information may not be captured, retained, communicated, transmitted, displayed or printed in whole or in part, except where required by law, and/or in accordance with the standards outlined in this policy. For example, because MTSU is a public institution, some PII may be subject to disclosure pursuant to the Tennessee Public Records Act (T.C.A. § 10-7-101 *et seq.*). In addition, the University may disclose information to third parties when such disclosure is required or permitted by law.

The information assets of the University, including the network, the hardware, the software, the facilities, the infrastructure, hard-copy documents and any other such assets, must be available to support the teaching, learning, research and administrative roles for which they are created. The University strives to employ appropriate physical and technical safeguards without creating unjustified obstacles to the conduct of the business and research of the University and the provision of services to its many constituencies in compliance with applicable state and federal laws. As a result, the University has

developed an Information Security Tutorial designed to educate University employees on the safeguards and procedures available to protect the University's information assets.

This policy serves as a companion to the MTSU Information Technology Resources Policy.

II. Policy Development and Maintenance

This policy was drafted by the Information Security Task Force, and forwarded to the University Vice Presidents and President for final review and approval. This policy shall be reviewed by the Information Security Task Force or any superseding University committee on at least an annual basis and any revisions shall be forwarded to the University Vice Presidents and President for approval.

III. Scope

MTSU maintains records to carry out its educational mission. Federal and State laws and regulations govern access to these records. This policy and related procedures are established to ensure compliance with these laws and regulations and to protect the integrity of University records and the privacy of individuals. This policy applies to all University students, faculty and staff, affiliates, third-party support contractors, and all others granted access to MTSU information assets. The policy applies to the use of PII including SSN whether that information is maintained, used or displayed wholly or in part, and in any data format, including but not limited to oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or other medium as determined.

IV. Definitions

A. Personally Identifiable Information (PII) is any information which can potentially be used to uniquely identify, contact, or locate a person. Under Tennessee law, "personal information" means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted: (i) social security number; (ii) driver license number; or (iii) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Tenn. Code Ann. § 47-18-2107(3).

1. Public/directory information. Some information that is considered to be PII is available in public sources such as telephone books, public websites, university listings, etc. This type of information is considered to be public/directory PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. Public/directory information is available to the public via the Tennessee Public Records Act and other laws. For guidance on student directory information, contact the registrar's office and/or review the undergraduate catalogue: Student Access to Educational Records.

2. Non-public/confidential information. All personally identifiable information except that information defined as directory/public information, unless the student has designated his/her directory/public information confidential. MTSU's requirement to protect non-public/confidential PII is largely governed by law or contract (e.g. HIPAA, FERPA, GLBA, human subject data, Tennessee Public Records Act, etc.). Examples include, but are not limited to, SSN, credit card numbers, health records, human subject data, bank account numbers, certain employment records and all FERPA non-directory information about students and former students.
 - B. SSN may be interpreted to include Taxpayer Identity Number (TIN).
 - C. Individual Workstations: Includes, but is not limited to, desktops, laptops and PDAs.
 - D. Removable or Transportable Media: Includes but is not limited to paper forms, reports, cassettes, CDs, USB tokens, flash drives, hard drives and zip drives.
 - E. Enterprise Systems: The term is applicable to any infrastructure as a means of describing its importance to the University's mission and how it should be administered, protected and funded. From a functional viewpoint, an Enterprise System will be either (a) the only delivery platform for an essential service, or (b) a platform for a service to a very broad constituency spanning organizational boundaries. An enterprise system is most frequently administered and protected by an institutional unit with expertise in both the technology and the business functions delivered.
 - F. MTSU ID Number: Middle Tennessee State University has created a unique identifier sometimes referred to as the "M-Number" to reduce the need for using the SSN in most business processes including instruction. Unique MTSU ID Numbers are assigned to all students and employees of the university and are not reused.
 - G. Departmental Information Security Contact: An individual identified within each department of the university to serve as the point of contact with respect to information security related issues within the department. The academic department chair, budgetary head, or his/her designee shall serve in this capacity, and this person is responsible for the definition, management, control, integrity or maintenance of a departmental or enterprise data resource. However, each individual is responsible for protecting their own PII.

V. Standards

- A. The University does not permit the use of PII as a primary identifier for any person or entity in any information system, except where the PII is required by law, and/or permitted by University policy. Prior to using PII, users are required to complete the Checklist for Usage of PII (Appendix 3) and file the Checklist with the appropriate Departmental Information Security Contact.
- B. Except where the SSN is required by law, the MTSU ID Number replaces use of the SSN and will be used in all electronic and paper data systems and processes to identify, track, and service individuals associated with the University. The MTSU ID Number will be permanently and uniquely associated with the individual to whom it is originally assigned.

- C. Where required by law and University policy, SSN may be stored as a confidential attribute associated with an individual and may be used as an optional key to identify individuals for whom a primary identifier is not known.
- D. Where the collection and use of PII including individual SSN is permitted by university policy, but not required by applicable law, the collecting entity shall use and collect such information only as reasonably necessary for the proper administration or accomplishment of its respective business, governmental, educational and medical purposes.
- E. Individuals shall not be required to provide PII, including SSN, verbally or in writing, at any point of service, nor shall they be denied access to those services should they refuse to provide PII, except where the collection of that information is required by law or otherwise permitted by University policy. A department's request that an individual provide their PII for verification of the individual's identity where such information has already been disclosed in accordance with this policy does not constitute a disclosure for purposes of this Policy. Questions about whether a particular use is required by law or permitted by policy should be directed to either the department chair, budgetary head, or the Departmental Information Security Contact who will be responsible for consulting with the Office of the University Counsel with respect to the interpretation of law or policy.
- F. Where the collection of SSN is required by law or permitted by University policy, all university departments shall inform individuals of their federal privacy rights when they collect such information.
 - 1. In the first instance where a department requests that an individual disclose his or her SSN, it shall provide the notice required by Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 552a), which requires that the individual be informed whether the disclosure is mandatory or voluntary, by what statutory or other authority the number is solicited, and what uses will be made of it. A subsequent request for production of a SSN for verification purposes does not require the provision of another notice.
 - 2. The notice shall use the applicable text from Appendix 2 of this Policy or such other text as may be approved by the Departmental Information Security Contact who shall consult as needed with the Office of the University Counsel with respect to the interpretation of law and ITD personnel with respect to technical implementations of the statement.
 - 3. It is preferable that the notice be given in writing, but in rare circumstances it may be necessary to give the notice orally, in which case procedures shall be described on the approval form to collect SSN as documentation that the notice is properly and consistently given.

- G. All newly developed or acquired application software will not be used to collect or store or transmit PII as data elements until a business requirement is submitted and approved by the appropriate Departmental Information Security Contact, University Counsel, ITD, and/or other authorities as deemed appropriate.
- H. All proposed contracts that involve the transfer, storage, and/or electronic recording of PII must be reviewed and approved by ITD to ensure appropriate technical controls and best practices are accounted for before the contract is signed.
- I. Access to servers housing databases or records containing PII must be restricted to permit only the access needed for the use and support of that application. The server must be protected by an ITD approved firewall, and other technical security measures as deemed appropriate by ITD.
- J. Where possible, all records containing PII shall be stored on secure network drives with access limited to those individuals or entities that require access to perform a legitimate University function. Individual workstations, laptops, mobile storage devices and other personal computers (e.g., PDAs and home computers, etc.) shall not be used to store records containing PII except where permitted by policy.
- K. All removable or transportable media (e.g., paper forms, reports, cassettes, CDs, USB drives, etc.) containing PII must be physically secured when not in use. Reasonable security measures depend on the circumstances, but may include locked file rooms, desks, and cabinets. Reasonable efforts must be made to encrypt portable devices which store PII.
- L. Subject to applicable document retention policies or unless required by law, when no longer required, paper documents and electronic media containing PII will be destroyed or disposed of using methods designed to prevent subsequent use or recovery of information. NOTE: ALL evidence subject to a litigation hold must be retained in whatever format the information is in and in whatever classifications in spite of otherwise general policies on retention.
- M. PII will be released to entities outside the University only where required by law, for University business necessity or with the express written permission of the individual or entity. Individuals with access to PII within the University's electronic information systems may need to consult with ITD personnel regarding the technical implementation of the disclosure/release of such information.
- N. All requests for information under subpoenas, court orders, compulsory requests from law enforcement agencies, etc. should be referred to the Office of the University Counsel before releasing any records. Records should only be released after consultation with the University Counsel.
- O. The University will limit access to records containing PII to those individuals requiring access as determined by job function. Individuals permitted access to PII will be instructed on the appropriate handling, protection, and destruction of this data by their management or designated representative.

VI. Procedure

Individual business units are responsible for the development, documentation and implementation of applicable procedures to effectuate this policy. The Departmental Information Security Contact is responsible for informing new departmental personnel regarding the MTSU Information Security Policy. Procedures are subject to review by Information Security Task Force or its successor.

VII. Incident Reporting and Response

Any member of the University who has knowledge of any evidence of PII being compromised or who detects any suspicious activity that could potentially expose, corrupt or destroy PII must report such information to the Departmental Information Security Contact. The Departmental Information Security Contact will in turn report the information to his/her supervisor, ITD, University Counsel, and the appropriate Vice President.

VIII. Non-Compliance

Violation of this policy may result in one or more actions, including but not limited to:

- A. The immediate suspension of network access, access to administrative systems, and access to the Internet.
- B. Use of the regular disciplinary processes and procedures of the University for students, staff, administrators, and faculty.
- C. Students may be recommended for suspension or expulsion from MTSU. Employees may be recommended for termination from MTSU employment.
- D. Referral to appropriate law enforcement agencies in the case where violation resulted in a suspected breach of sensitive information.
- E. Personal liability for willful violation of this policy resulting in loss to the University.

IX. Approved Uses of SSN

University offices may not collect SSNs for purposes other than those noted in Section V, Standards.

The primary uses and reasons for the continued capture, storage, retention and processing of SSN data are identified and documented in the Approved Uses of SSNs - Appendix 1. Typically, processes that access historical SSN data, or require or permit continued use of SSN data, are described here. Additional processes may be added to the appendix by contacting the Information Security Task Force or its successor.

APPENDIX 1

Information Security Policy

Approved Uses of SSNs and Other Personally Identifiable Information

The primary uses and reasons for collecting SSNs and other personally identifiable information include, but are not limited to, the following:

- **Enrollment:** Those wishing to enroll in academic offerings at Middle Tennessee State University (MTSU) - both credit and non-credit - are required to provide a social security number (SSN) for secondary identification purposes. IRS regulations do require the University to request a SSN as a Taxpayer ID number for use in tax reporting. In addition, any student applying for financial aid must provide a SSN to the University.

If a person enrolling in a University academic offering - credit or non-credit - refuses to provide a SSN, certain services, such as transcripts, enrollment verification, tax reporting, financial aid and other services may not be available to the individual, and MTSU cannot guarantee a complete academic record for the individual.

Historic records may contain a student's SSN, as SSN was previously used as the primary identifier.

- **Employment:** A SSN must be provided on I-9's in accordance with the Immigration Reform and Control Act of 1986 (IRCA), as overseen by the Human Resource Services .
- Any person employed by the University must provide a SSN as the taxpayer ID number as directed by the IRS. This includes all employees, including part-time and student employees. Providing the SSN is a condition of employment. Applicants for employment must also provide a SSN, if requested, for mandatory background checks.
- **Employee Benefits:** If required by a benefits provider, the SSNs of dependents/beneficiaries may be collected to receive service. The University may also release an employee's SSN to benefit providers.
- **Payment for Personal or Professional Services:** Any person providing services to the University as a independent contractor, invited speaker (honorarium) or research subject for which payment will be made, must provide a SSN as the taxpayer ID number per IRS regulations. These taxpayer ID numbers will be stored in the accounting system as part of the vendor record.
- **Planned Giving Donors:** Donors participating in planned giving programs must provide a SSN as the taxpayer ID per IRS regulations.

- **Insurance Providers:** The SSNs of faculty, staff and students continue to be the patient identifier for many health care providers. For example, to enable payment of medical bills, student SSNs are shared with the insurance company providing health coverage.
- **Third Party Sponsors:** Various third-party sponsors of student aid, including several state agencies, require the submission of SSNs for those students in which aid is being provided. In order for the sponsor to make payment to the university, a SSN must be provided for proper verification.
- **Credit Card Information:** Under current Payment Card Industry (PCI) standards, merchants are allowed to maintain customer credit card numbers for a period of time after the transaction has occurred. The allowable time is set in the PCI standards and subject to change periodically.
- **Advancement Services:** SSN is required for certain tax documents. For example, form 8282-Donee Information Return, requires a donor's SSN for gifts of tangible property valued over \$5,000 and sold within two years of the receipt of the gift. Also, donors who make gifts of life insurance may be required to provide a SSN as dictated by the particular insurance company. Historical documents and related databases may contain SSNs since they were previously used as primary identifiers.
- **Student Health Services:** SSN may be employed as patient identifier for referrals and consultation with outside medical providers and for communication with insurance companies.
- **University Police:** Department personnel collect SSN data during an arrest as required by the Tennessee Bureau of Investigation (TBI) and Federal Bureau of Investigation (FBI). Additionally, UP maintains copies of fingerprint cards that contain SSN data, and the "arrest" module of the records database stores SSN data.

APPENDIX 2

Information Security Policy

Sample Disclosures

General mandatory disclosure.

Disclosure of your social security number (“SSN”) is required of you in order for Middle Tennessee State University to [state intended use of SSN] , as mandated by [Federal] [State] law. Further disclosure of your SSN is governed by the Tennessee Public Records Act and other applicable law.

General voluntary disclosure.

Disclosure of your social security number (SSN) is requested from you in order for Middle Tennessee State University to [state intended use of SSN] . No statute or other authority requires that you disclose your SSN for that purpose. Failure to provide your SSN, however, may result in [state what may happen if the individual fails to provide SSN] . Further disclosure of your SSN is governed by the Tennessee Public Records Act and other applicable law.



APPENDIX 3
Information Security Policy

Checklist for Usage of PII

PII User Name _____ Date _____
Department _____ Phone _____
Address _____ E-Mail _____

Form with 7 sections: 1. Briefly describe the type of PII proposed to be collected and why it is required. 2. Briefly describe the process used to collect the PII information. 3. Describe how the PII will be stored including the types of media used for both primary and backup storage and what security measures will be employed. 4. Will the data be stored on any portable equipment or media? If so, please describe how this will be used and what type of security measures will be used. 5. Will any PII data be used as a primary identifier? 6. List the approximate number of individuals requiring access to the PII data retained by this system by classification. (Table with columns: Faculty, Staff, Students) 7. Describe the method(s) used to access the data and what controls will be implemented to manage that access.

Please file with the Departmental Information Security Contact.

PII User Signature _____

Date _____

Departmental Information Security Contact Signature _____

Date _____