Tennessee Technological University
Policy No. 856

Data Security and Handling Policy

Effective Date: August 15, 2017

Policy No: 856
Policy Name: Data Security and Handling Policy
Policy Subject: Data Security and Handling

I. Purpose

This policy describes the requirements and standards for securing Tennessee Tech data and its handling.

II. Review

This policy will be reviewed every two (2) years or whenever circumstances require review, whichever is earlier, by the Chief Information Security Officer, with recommendations for revision presented to the Information Technology Committee and University Assembly.

III. Policy

All users of data must adhere to the requirements applicable to each data classification as defined by TTU Policy 855 (Data Classification).

IV. Data Security & Visual Identifiers (Labeling)

A. Level I: Public Information: Information in this category does not require any colored marking or notation and should have no manner of restriction in its distribution or handling.

B. Level II: Internal Information: Information in this category must be marked or denoted with a heading reading "Level II: Internal" in a purple color. When stored or transmitted electronically, Internal Information is not required to be encrypted, but access must be limited to employees or contracted workers conducting Tennessee Tech business. Internal Information must not be transferred, transmitted, or disseminated externally, except on official business, and must follow security best practices.

C. Level III: Confidential Information: Information in this category must be marked or denoted with a heading reading "Level III: Confidential" in an orange color. When stored or transmitted electronically, Confidential Information must be encrypted at AES 128-bit encryption. Access to Confidential Information must be restricted to Tennessee Tech-managed accounts. Information in a non-electronic format must be secured in a locked location when not in use. Distribution of Confidential Information should only be on a need-to-know basis.

D. Level IV: Sensitive Information: Sensitive Information must be marked or denoted as such with a heading reading "Level IV: Sensitive" in a red color. When stored or transmitted electronically, Sensitive Information must be encrypted at the highest available level, preferably AES 256-bit encryption or higher. On systems where AES 256-bit encryption is not available, the minimum acceptable encryption is AES 128-bit encryption, unless an express written

exception is obtained from the Chief Information Security Officer or his/her designee. Access to information must be restricted to Tennessee Tech-managed accounts. Sensitive Information in a non-electronic format must be secured in a locked location when not in use. Distribution of Sensitive Information should only be on a need-to-know basis.

E. All encryption requirements must, absent good cause, adhere to the current relevant National Institute of Standards & Technology (NIST) policy. The Chief Information Security Officer must approve in writing any exception to this requirement.

V. Data and Media Reassignment and Destruction Handling

A. Level I: Public Information: Media devices with Public Information must be erased using minimal procedures and security best practices. A single-pass of zeros or random bits must be executed before returning the media device to a working state. Non-electronic media with Public Information should have no restriction in its handling or destruction and should be recycled, where available.

B. Level II: Internal Information: Media devices with Internal Information must be erased using NIST standard procedures and security best practices. A three-pass or Department of Energy (DoE) procedure is the minimum required procedure before returning the media device to a working state. Destruction of media is not required unless circumstances require otherwise or media is inoperable. Non-electronic media with Internal Information must be disposed of via secure document disposal, such as a secure shredding service, or be destroyed using a cross-cut paper shredder.

C. Level III: Confidential Information: Media devices with Confidential Information must be erased using NIST standard procedures and security best practices. A seven-pass or Department of Defense (DoD) procedure is the minimum required procedure before returning the media device to a working state. Destruction of media is not required unless circumstances require otherwise, media is inoperable, or media is assigned to designated Tennessee Tech personnel. Media under warranty may not be returned to the manufacturer unless the data has been erased using the above-mentioned procedure. Non-electronic media with Confidential Information must be disposed of via secure document disposal, such as a secure shredding service, or be destroyed using a cross-cut paper shredder.

D. Level IV: Sensitive Information: Media devices with Sensitive Information must be erased using NIST standard procedures and security best practices. A seven-pass or Department of Defense (DoD) procedure is the minimum required procedure before returning the media device to a working state. Destruction of media is required in all cases where used and may not be surplused or recycled. Media may not be returned to the manufacturer under any circumstances. Non-

electronic media with Sensitive Information must be destroyed using a cross-cut paper shredder or reduction of the media to a pulp form.

E. If the media device's data classification is unknown, Level IV procedures must be followed.

VI. Implementation

The labelling requirements of this policy do not apply to information created prior to January 1, 2018.

VII. Interpretation

The Chief Information Security Officer or his/her designee has the final authority to interpret the terms of this policy.

VIII. Citation of Authority for Policy

T.C.A. § 49-8-203(a)(1)(E)

Approved by:

Information Technology Committee: September 7, 2017

University Assembly: November 29, 2017

Approved by the President on August 15, 2017, pursuant to Policy 101, Section VII.A.