UA Local 290 Apprentice and Journeyman Training Institute
Data Security Plan
Use, Storage or Transmission of Electronic Data

I. Objectives:

Pursuant to regulations of the US Department of Education, UA Local 290 Apprentice and Journeymen Training Institute (AJTI) is charged with protecting the privacy of students and maintaining the confidentiality of data. This policy provides standards for data security plans involving the storage of electronic data constituting Sensitive Data. The intent of this policy is to ensure that the protection of the privacy of students and employees and ensure the confidentiality of data in accordance with the Family Education and Privacy Rights Ace (FERPA).

1. Sensitive Data

   Pursuant to the Data Classification Policy, Sensitive Data is defined as follows:

   "Sensitive Data: any information protected by federal, state and local laws and regulations or industry standards, such as HIPAA, the Health Information Technology for Economic and Clinical Health Act (HITECH), the U.S. Family Educational Rights and Privacy Act (FERPA), and similar state laws.

   For purposes of this Policy, Sensitive Data include, but are not limited to:

   1. Personally Identifiable Information (PII): any information about an individual that (a) can be used to distinguish or trace an individual's identity, such as name, date and place of birth, mother's maiden name or biometric records (b) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization could result in harm to that individual and (c) is protected by federal, state or local laws and regulations or industry standards.

   2. Protected Health Information (PHI): any information processed, transmitted or stored by a Covered Entity (as defined in HIPAA) that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for health care and (a) identifies the individual or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

   Examples of Sensitive Data
   Examples include, but are not limited to, any information concerning a person that can be used to identify such l person, such as name, number, or other identifier, in combination with any one or more of the following:
   - Social security number
   - Driver's license number or non-driver identification card number
   - 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
   - Email address with password

- Name
- Geographic subdivision smaller than a state
- Any element of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date or date of death
- Telephone number
- Fax number
- Electronic mail address
- Social security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/License number
- Vehicle identifier and serial number, including license plate number
- Device identifier and serial number
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Biometric identifier, including finger and voice print
- Full face photographic image and any comparable image
- Any other unique identifying number, characteristic, code or combination that allows identification of an individual.

II. Activities to Achieve the Objectives:

The following methods of storing electronic research data containing Sensitive Data are acceptable:

1. Server Based Systems:
   The data is stored on a server in compliance with the UA Local 290 Apprentice and Journeymen Training Institute Policy.

2. Endpoints:
   The data is stored on an Endpoint (such as an external drive) in compliance with the policies referenced above.

3. Data Transmission:
   An acceptable data security plan must provide that all electronic transmissions of Sensitive Data over the internet (including by email), file transfers or other data transfer modalities, are made in compliance with the Email Usage Policy described in the Employee Handbook.

4. Data Loss/Security Breach:
   Any loss of or breach of security relating to research data containing Sensitive Data must be re- ported to the Director as an unanticipated problem involving risks to subjects or others.

   Examples of security breaches include:
   - Lost or stolen desktops, laptops, USB drives, CD/DVD/Zip drives, etc. with stored data.

- A compromised account that is used to look up data (e.g., unauthorized user has had access to the account).
- A compromised work station or server that contains data.
- Accidental disclosure or data to unauthorized recipients (e.g., sending data to an incorrect email address).

III. Roles & Responsibilities:

All employees are responsible to follow this data security plan to ensure our apprentices sensitive data is secured. It is their responsibility to report any data loss/security breach to the Director of Training immediately.

IV. Guidelines for Review & Evaluation:

This Data Security Plan has been in effect since January 1, 2017. It will be reviewed and evaluated annually by the Institutional Advisory Committee and JATC. Faculty and Students are encouraged to participate in the evaluation of this Data Security Plan.