Safeguarding of Customer Information

Introduction and Purpose

This policy is being introduced as required by the Federal Trade Commission under the Gramm-Leach-Bliley (GLB) Act.

At Installer Institute, safeguarding the privacy and confidentiality of personal information is important. As a licensed, accredited education and training institution, we collect, retain, and use personal non-public information about individual students and staff members. We may collect personal information from such sources as hard copy applications, electronic forms, or over the Internet. The objectives of our information security program are to ensure the security and confidentiality of such personal information; to protect against any anticipated threats to its security or integrity; and to guard it against unauthorized access or use.

Any sharing of nonpublic personal information about our students or employees must be done in strict adherence to the Federal Family Educational Rights and Privacy Act (FERPA) guidelines. The school may exchange such information with certain nonaffiliated third parties (under limited circumstances) to the extent permissible under law. Examples may include (but are not limited to) accrediting organizations, state or local, state & local authorities if required by state statutes, officials in cases of health & safety emergencies, and appropriate parties in connection with financial aid.

We restrict access to student and employee information only to those employees who have business reasons to know such information, and we educate our employees and contract service providers about the importance of confidentiality and privacy.

Policy

In order to provide adequate safeguards over customers' information, Installer Institute adheres to the following minimum technical specifications:

- Any computer device on Installer Institute's network that makes non-personal public information available must be certified secure.
- Customer information, including credit card data, must be reasonably secured against disclosure and modification as determined by Installer Institute policy.
- Installer Institute must oversee local and contracted service providers by taking steps to select and retain providers that are proven capable of maintaining appropriate safeguards for customer information.
- Installer Institute will contractually require service providers to implement and maintain such safeguards; and
- Installer Institute will periodically evaluate, based on results of testing and monitoring,

any material changes to the service providers' operations.

Installer Institute may accept payment by credit card when approved by the student or party making payment on behalf of the student. Procedures for timely deposit of credit card transactions and safe and proper handling of the data are followed.

IT will review the Installer Institute's hardware and software to ensure that the server is secure and the program requirements have been adhered to. (See Procedures below).

The following safeguards need to be in place:

- Personal computers containing confidential information must be secure.
- Adequate internal controls regarding separation of duties must be in place.
- It is Installer Institute's responsibility to maintain the customer's credit card or e-mail information in a confidential manner.
- Any hard copy documents containing confidential information must be shredded in a timely manner.

Procedures

1. Approvals – Obtain approvals from the School Director
2. Program Requirements – IT is responsible for these procedures to establish a secure computing environment.
    a. Install and maintain an effective network firewall to protect data accessible via the Internet.
    b. Keep operating system and application software security patches up-to-date.
    c. Encrypt stored data.
    d. Encrypt data sent across open networks.
    e. Use and regularly update anti-virus software.
3. Develop adequate office procedures for staff or contract service providers to maintain secure information.
    a. Restrict access to data by business "need-to-know".
    b. Assign a unique ID to each person with computer access to data.
    c. Do not use vendor-supplied defaults for system passwords and others security parameters.

d. Track access to data by unique ID.
e. Regularly test security systems and processes.
f. Maintain a policy that addresses information security for employees and contractors.
g. Restrict physical access to cardholder information.

Internal Controls

Segregation of duties is important to protect against fraud and maintain confidentiality.

1. Individuals who collect monies and/or write receipts may not be the same individuals who account for deposits.
2. Different Individuals are to perform the following functions:
    a. Collecting monies and preparing receipts
    b. Depositing receipts
    c. Accounting for receipts
3. Limit access to information such as ID and credit card numbers only to those individuals who need to know.
4. Protect and shred confidential information.
5. Small departments that do not have sufficient staff to meet ideal segregation of duties requirements must ensure that detailed supervisory review compensates for this weakness.