UNITECH TRAINING ACADEMY

Plan for Technical Infrastructure and Data Security

Purpose

The purpose of this plan is to establish guidelines for the technical infrastructure and ensure the privacy, safety, and security of data contained within the technical infrastructure of Unitech Training Academy's networks.

Responsibility

The Corporate Director of IT is responsible for the administration of this plan.

The Corporate IT Department supports operation at all campus locations of Unitech Training Academy. The main data center is located in Lafayette, Louisiana while each individual site is supported with an onsite server/data room and backup capabilities.

Third party assistance may be requested for maintenance items above and beyond the scope of ability or resources.

Procedure

Unitech Training Academy is committed to providing employees with equipment and supplies needed to promote efficient processing of student records in all area of the campus. Unitech Training Academy provides data security using a role-based network design. The basic premise of a role-based network design is to construct barriers between system users and the system's data. Based upon their job functions, only authorized/authenticated users may query data and access files on secured systems.

When employees are hired, The IT Department personnel receive notification from Human Resources to create network accounts and configure security and access to various electronic systems. Access is granted as needed to perform respective job functions.

To ensure all personnel are aware of and comply with all of the requirements to protect and secure data, Unitech Training Academy has established the following security measures:

- Access to the internal server is granted to the Campus Director. Specific rights are assigned to each user. A username and password is required to access the internal server.
- Access to Diamond SIS software is granted only upon approval by the Campus Director and IT department.
- Data security is addressed during employee orientation and employees are made aware of the confidentiality agreement within the handbook

Plan for Technical Infrastructure and Data Security

Unitech Training Academy staff makes every effort to ensure the privacy, security, and safety of all data stored on premise as well as external to the institution. Unitech's Corporate IT Department takes all potential threats seriously and addresses these threats as they arise.

To ensure adequate and continued operation of the institution's technical infrastructure:

- Computer hard drives are backed up to the internal server on nightly basis. The internal server is backed up to an external USB attached hard drive on a nightly basis.
- A full backup of our student management system (Diamond SIS) is copied to a network storage device offsite each night.
- Each internal servers data files are backed up on a weekly basis to a network storage device located offsite.
- Diamond SIS is housed on an internal server at each campus maintained by the company and backed up nightly. Access to Diamond SIS is granted based on the established privileges assigned to each employee's user name. Password are required to enter the Diamond SIS server and the database system (two layers of security)
- Individual computers also require passwords to gain access to the hard drive.
- File transfers are complete utilizing an FTP site with limited access based on position
- The National Student Loan Database System (NSLDS) is used for enrollment reporting and monitoring lifetime award limits. The Common Origination and Disbursement (COD) system is used to monitor award information (individual and institutional), MPN status, entrance counseling, and PLUS credit decisions. Both COD and NSLDS are web-based software sponsored by the U.S. Department of Education. An FSA user id, password, and two-factor authentication token are needed to access COD and/or NSLDS

Network and Hardware Reliability

Unitech Training Academy supports a full spectrum of wired and wireless access at each site. Remote sites are tunneled back to the main campus using either dark fiber or over the wide area network. By designing the network in this manor, it provides a more effective method of management and security and provides for access to data from all campus locations remotely. Access to each campus' physical network from the outside is only allowed by Virtual Private Network (VPN). Once the VPN connection is established, remote user access to data occurs as if they were located at that campus.

An active failover device for crucial services such as firewalls, wireless controllers, and servers are used to ensure reliability and access for students and staff. A redundant power supply has also been

installed in each device to eliminate a single point of failure. Devices which are less critical in the network and are covered by a limited lifetime warrantee are used and replaced as needed.

Power to operate all devices are protected and conditioned by uninterruptible power supplies at all campus locations. A backup power supply is in place provide additional backup power to ensure services uptime and data integrity. The Corporate IT Department provides monitoring for all servers and data infrastructure, and is available to handle major emergencies when these may arise.

Backup Procedure

The backup system currently contains three backup levels. The first backup level is a script that is run weekly for each server's date files. This script runs a mirror comparison that will push updates to the current data on each server to the archived data that is located on our network storage device at an offsite location. The second backup level is another script that runs a full backup of the student database (Diamond SIS) and copies it to the network storage device located off site. The third backup level will be a full bare metal backup of each server. This backup is run every night on all servers and is stored on a local USB attached external hard drive.

Technical Infrastructure and Data Disaster Recovery

In the event of a disaster which would impact technical resources and operations, documentation and system backups are in place to reinstate all critical data. Use of a secondary virtual array allows Unitech Training Academy the option to reinstate mission critical servers at a different location in the event of a disaster scenario.

Physical Assets Maintenance and Replacement

Each year, the Corporate IT Department reviews the technical infrastructure and computing hardware along with the Chief Operations Officer to determine how to allocate funds in the most efficient and effective manner. Network infrastructure is added or replaced as required to ensure students and staff have access to all services and data.

Learning Resource Center

Each campus will house a Learning Resource Center to provide student access to computers with network capabilities and the ability to print. The Learning Resource Center will be remotely managed by the Corporate IT Department and updates will be made to equipment accordingly. Students are granted access to the LRC during normal business hours.

State Law and Federal Codes Compliance

Unitech Training Academy is committed to remain compliant with any and all regulations set forth by the Department of Education's Program Participation Agreement (PPA), Student Aid Information Gateway (SAIG), and the Council on Occupational Education.

Access to Educational Records and Data

Educational Records are all files, records, or documents maintained by the school, which contain information directly related to the student. The only persons allowed access to such records are those personnel who have a legitimate administrative or educational interest. Student must request in writing, if not in person, authorization for all or part of their records.

Under the authority of the Family Educational Rights and Privacy Act of 1974, a student has the right to examine certain files, records or documents maintained by the school, which pertain to them. The school must permit a student to examine such records within 45 days after submission of written request, and to obtain copies of such records upon payment of the cost of reproduction.

Evaluation

Evaluation of data security measures is a continual process. Any irregularities with data systems are immediately brought to the attention of the Corporate Director of IT who will review network firewalls and IP addresses attempting to access the internal server. In the event of a data breach, the incident to the will be reported to the Department of Education.

Student are surveyed periodically on the availability of media services which is driven by the technical infrastructure of the institution. The Plan for Technical Infrastructure and Data Security is available to students through the Unitech Training Academy website and is available to employees through the UTA Portal.

The Corporate Director of IT and Student Affairs team will evaluate the plan each year and revise as needed.