Cyber Security

Overview

As a subsidiary of Nelnet, Inc. (NYSE: NNI), FACTS adheres to the highest levels of security and compliance standards in the industry to ensure the confidentiality and integrity of all customer information. We make it a priority. The MSDE, your participating schools, and families can rest assured they are receiving services and technology that are compliant with current federal and state-specific regulations.

All FACTS solutions are fully hosted and data transmission is encrypted using SHA-256. No payment account information is captured, stored on, or transmitted from Institution applications All FACTS solutions are PCI-DSS Level 1 Certified and fully compliant with all regulations.

Our operations are connected via a meshed network with our data center in Bellevue, Nebraska. Our Disaster Recovery facility is located in Sioux Falls, South Dakota. All student information transmitted from the Institution's system is securely sent and received using encrypted SFTP or TLS channels. Data files are always exchanged using the encrypted SFTP protocol. In addition, we recommend that files transferred be encrypted using the PGP protocol. Real-time data integration uses web services that are secured using industry standard TLS encryption.

We also partner with PaymentSpring for a tokenization system to store and process credit cards for payment purposes. PaymentSpring is hosted at Amazon Web Services (AWS), which is a PCI Level 1 Compliant cloud storage solution.

FACTS currently contracts with TierPoint, a Level 4 regional collocation and data center. TierPoint is responsible for all physical security and environmental protection of the primary and back up data centers. Access to the Nelnet cage within the data centers is maintained by Nelnet on a system independent from TierPoint. Nelnet's caged facility is monitored by cameras with recorded data stored on internal servers for 90 days. Monthly physical inspections are performed to ensure that no wireless access points have been attached to Nelnet equipment. TierPoint's physical and environmental controls are tested as a part of annual SSAE-16 / SOC1 testing.

We view PCI compliance as a year-round requirement. Our PCI environment is segmented from other environments. Vulnerability scans and penetration tests are done more frequently than required by PCI regulations. We have standards and controls in place to monitor for and protect against security breaches. In addition, our Quality Control and Compliance department regularly reviews controls tested for PCI requirements to ensure controls are maintained throughout the year.

Finally, all FACTS systems are routinely audited by both internal and external resources. Our Compliance Officer works with the Network to team on the annual PCI Audit and SOC-1 reporting and we contract with an outside QSA firm (Trustwave) for penetration testing and outside scans. Our systems are monitored constantly via monitoring stations in Nebraska, California, and Hong Kong for CPU utilization and response time. We maintain detailed activity logs for audit trail purposes.