FACTS
A nelnet Company

Data Security, Compliance, and Business Continuity

Protecting Your Data, Supporting Your Systems

Security

FACTS has detailed security standards that are regularly assessed, reviewed, and tested for education and efficacy.

Application Security and Encryption

Teams across our company are responsible for staying current on innovations and trends in school technology and data security. They help us maintain multiple security certifications from organizations like the Computing Technology Industry Association (CompTIA), Disaster Recovery Institute (DRI) International, Information Systems Audit and Control Association (ISACA), International Information System Security Certification Consortium (ISC2), the ITIL Foundation, and the Payment Card Industry (PCI) Security Standards Council.

Cybersecurity

Our data network infrastructure has a number of security measures in place to predict issues, protect information, and keep your school compliant. Intrusion detection and prevention systems (IDS/IPS) monitor all inbound/outbound activity and help protect against denial-of-service (DoS) attacks. We also perform regular external and internal scans of our network and network devices to look for issues, updates, or changes to the configuration.

Testing and Threat Assessment

We follow strict, secure coding guidelines throughout the software development lifecycle. Trained developers perform manual/automated coding reviews and we perform vulnerability scans and penetration testing methods such as:

- PCI Pen Testing
- Vulnerability scans and penetration testing:
  - PCI Pen Testing 3.2 standards (including Application Security Review)
  - Internal, external, and web application penetration testing
  - Network segmentation testing
  - Red/blue team testing

Physical Security

Tabs are kept tight on things like building entrances and data centers. Security cameras, controlled access to buildings and sensitive rooms, and certain physical authentication methods make sure that the only people near our data centers are the ones who are supposed to be.

Learn more at FACTSmgt.com/security-compliance

SSAE 18 AUDITED

PCI DSS Level 1 VALIDATED

FACTS
A nelnet Company

Compliance

We know that managing sensitive personal and financial information is important to your school. At FACTS, we have a strong, long-standing commitment to security, compliance, and data protection.

GDPR and Data Protection

Striving to provide superior customer service, FACTS places great emphasis on its customers and their privacy rights. In doing so, FACTS will comply with European Union Privacy Directives, most notably the EU General Data Protection Regulation. See more information about FACTS' compliance with GDPR, CCPA, and other data privacy provisions at FACTSmgt.com/privacy-policy.

SSAE 18 Audited

The Statement of Standards for Attestation Engagement is an audit standard designed for third-party service organizations. The SSAE 18 results of vendor service organizations are used in audits of many institutions, and they address all aspects of the service organization's control environment. FACTS is SSAE 18 Audited on an annual basis.

PCI DSS Level 1

The Payment Card Industry Data Security Standards (PCI DSS, or more commonly, PCI) are a set of standards set forth by the four major card associations to protect cardholder data. All merchants and processors need to have physical, electronic, and procedural controls in place to ensure that cardholder data is stored and handled securely at all times. FACTS is PCI Level 1 compliant.

Internal Compliance Training and Testing

All of our associates (including the non-IT ones) regularly participate in phishing simulation tests, security awareness training, and professional development related to internal/external security.

Business Continuity

Disaster Recovery

We strive to prepare for anything. In the event of an emergency, our response plans involve clearly-defined processes and roles to make sure things get back to normal as quickly as possible. And because our multiple data centers have like-for-like network configurations, disaster recovery and failover scenarios are easier to follow.

Infrastructure, Reliability, and Redundancy

We contract with a Level 4 regional collocation and data center. In addition to our primary data center, we have a disaster recovery facility in place as a precaution. Each data center contains:

- ISP diversity
- SAN upgrades
- Device firmware/software updates
- Internal/external monitoring capabilities
- Dual firewalls
- IPS/IDS devices

Learn more at FACTSmgt.com/security-compliance

SSAE 18 AUDITED

PCI DSS Level 1 VALIDATED