# MHS Security Protocols and Continuity Assurance - Education

Protecting a district's student information and ensuring the safe, continuous availability of the wide range of applications implemented across the institution's different types of users and externally.

Hundreds of laws or acts require such measures to be implemented. Below is a list of some of the more commonly known laws enacted today:

- **FERPA** Federal - Family Educational Rights and Privacy Act
- **COPPA** Federal - Children's Online Privacy Protection Act
- **PPRA** Federal - Protection of Pupil Rights Amendment
- **CIPA** Federal - Children's Internet Protection Act
- **AB 1584** California, Assembly Bill No. 1584
- **SB 1177** California, Senate Bill No. 1177
- **SOPIPA** California, Student Online Personal Information Protection Act
- **HIPPA** Federal - Health Insurance Portability and Accountability Act
- **GDPR** EU, General Data Protection Regulation

The certified technical measures taken by MHS are among the highest found in and outside of education.

## Security and Continuity Measures

Below is a high-level summary of the security and continuity areas that are the focus of the MHS technical measures and third-party audits mentioned above.

- External Vulnerability Detection/ Remediation Measures
- Annual Third-Party Vulnerability Pen Testing
- Internal Vulnerability Measures
- Disaster Recovery Measures
- Horizontal Scalability Measures
- Source Code Vulnerability Measures
- Access Control Measures

### MHS Third-Party Audits and Certifications

To validate these efforts, MHS invests heavily in technical measures, continuous vulnerability testing, vulnerability mediation, and annual third-party certification audits. Below is a summary of MHS' third-party audits of industry standards of excellence certifications of security and continuity.

## ISO 27001

ISO 27001 refers to a globally recognized standard for managing information security. Formally known as ISO/IEC 27001, it is part of a growing family of ISO/IEC Information Security Management System (ISMS) standards, the "ISO/IEC 27000 series" that provides a framework for organizations to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

### Key Features of ISO 27001 certification requirements:

#### Information Security Management System (ISMS)

- At its core, ISO 27001 requires establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). This ISMS is an overarching management framework through which the organization identifies, analyzes, and addresses its information risks.

#### Risk Management

- The standard emphasizes a risk management process involving people, processes, and IT systems, ensuring a holistic approach to securing information.

### Security Controls

- ISO 27001 includes a set of recommended security controls categorized into different areas such as risk assessment, security policy, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management, and compliance.
- The 2013 version of the standard (currently the most widely used) lists 114 controls in 14 groups.

### Performance Evaluation

- The standard also requires continual monitoring and regular reviews of the ISMS's performance, apart from the initial setup. This helps in making continual adjustments to handle any new or evolving risks.

## SOC 2 Certifications

SOC 2 (System and Organization Controls 2) is a framework for managing data based on five "trust service principles"—security, availability, processing integrity, confidentiality, and privacy. It is an auditing procedure developed by the American Institute of Certified Public Accountants (AICPA) that ensures service providers securely manage data to protect the organization's interests and its clients' privacy. SOC 2 is particularly relevant to technology and cloud computing organizations that store customer data.

**Key Features of SOC 2 certification requirements:**

### Trust Service Principles

- **Security:** The protection of system resources against unauthorized access. Access controls help prevent potential system abuse, theft, or unauthorized removal of data, software misuse, and improper information alteration or disclosure.

- **Availability:** The system is available for operation and use as committed or agreed to. This principle involves the functioning of systems, network performance, and site failover measures.

- **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized. This principle addresses whether systems achieve their purpose (i.e., deliver the right data at the right price at the right time).

- **Confidentiality:** Information designated as confidential is protected as committed or agreed. Encryption is an example of a common method of ensuring confidentiality.
- **Privacy:** Personal information is collected, used, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice.

### Types of SOC 2 Reports

**Type I Report** describes a vendor's systems and whether their design is suitable to meet relevant trust principles.

**Type II Report** details the operational effectiveness of those systems over a specified period.

**For detailed information on MHS' compliance certifications and documentation, please visit:**

MHS.com/Compliance





MHS