"THE AXIOM DASHBOARD EMPLOYS A UNIFIED SECURITY MODEL, WHERE THE SECURITY THAT YOU ESTABLISH IS IN EFFECT ACROSS ALL CLIENTS."

aws
amazon web services

CYBERSECURITY

SSL
SECURE
SSL

OPERATIONAL RESILIENCE

The **AXIOM** DASHBOARD is built on the **AWS platform** which ensures real-time backups to protect your **DATA**. Full implementation and validation of ISO 27001 standard. AWS also aligns with the ISO 27017 guidance on **information security** in the cloud and ISO 27018 code of practice on **protection** of **personal data** in the **cloud**.

TWO WAY AES-256 ENCRYPTION

Upon opening an encrypted file, **AXIOM** employs a two-way **AES-256 encryption** that uses a composite key based on information from the machine to encrypt the password and secure it on the **server**. Connecting to the AXIOM Dashboard requires Secure Socket Layer (SSL) encryption of data between AWS Cloud and all clients. The server monitors access to the AXIOM Dashboard to disconnect idle users, and create backups of your data in real-time.

AES 256 ENCRYPTION

AUTHENTICATION

The platform **encrypts** credentials stored within solutions so the credentials are **protected**. AXIOM Dashboard generates digitally signed data and RSA keys to verify signed data. AXIOM Dashboard employs Secure Storage of container data (with Database Encryption enabled) AES-256 CBC mode.

FERPA COMPLIANCE

The **AXIOM** dashboard follows FERPA Compliance guidelines set by National Institute of Standards and Technology (NIST). It employs a **unified security model**, that adheres to NIST SP 800-122 controls and NIST SP 800-53. This ensures that students' **Personally Identifiable Information** (PII) remains secure, and **access** to data is provided on a **need** to know basis via SSL/TLS 1.2 **secured connections**.

ACCESS CONTROL

Our platform offers the ability to define permissions that determine **levels of access** to your solution.