IT Security and Privacy Statement

6/14/22

Smartest Edu, Inc., d/b/a Formative, places great importance on data privacy and information security in order to protect against external threats and malicious insiders. Formative's IT Security and Data Privacy strategy prioritizes detection, analysis, and response to known, anticipated, or unexpected threats; this strategy also emphasizes the effective management of risks as well as resilience against data incidents. Formative continuously strives to meet or exceed the industry's information-security best practices and applies controls to protect our clients and the organization. In addition to adhering to all applicable state, federal, and international privacy laws, Formative maintains a formal Privacy and Compliance Program structured around the following:

- U.S. Sentencing Guidelines: Seven Elements of an Effective Compliance Program
- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- General Data Protection Regulation (GDPR)
- ISO 27001
- System and Organization Controls (SOC 2)

For more information, please review this document, which provides an overview of Formative's Best-In-Class approach to information security, data privacy, and its practices to secure data, systems, and services.

Data Protection Safeguards

EMPLOYEE BACKGROUND CHECKS

Formative maintains a high level of ethical standards that are defined and enforced through Formative's code of conduct as well as the Privacy and Compliance Plan.

Formative requires confidentiality and nondisclosure from all those who work for and with Formative, both during and after engagement. All Formative employees undergo background checks and sign a non-disclosure agreement before hire. Formative carefully screens people who do work for, or on behalf of, the company.

Formative enforces disciplinary action for noncompliance with Formative policies.

EMPLOYEE PRIVACY & SECURITY AWARENESS TRAINING

Upon hire and on an ongoing basis, all employees are required to undertake privacy and security training, both of which cover privacy practices and the principles that apply to the proper handling of personal information, including (but not limited to) placing limitations on using, accessing, sharing, and retaining personal information.

We provide training on specific aspects of security that employees require based on their specific roles.

INCIDENT MANAGEMENT

Formative has a written Incident Response Plan that details the processes for detecting, reporting, identifying, analyzing, and responding to Security and Privacy Incidents that affect Formative Systems and Client Data.

VENDOR SELECTION & RISK MANAGEMENT

Formative Systems may use sub-processors to perform services; these sub-processors are only entitled to access customer data as needed in order to perform services and shall be bound by written agreements that require sub-processors to provide strict levels of data protection as required by Formative and all applicable regulations. For a list of our sub-processors, please review the “Third Parties” section in Formative’s Privacy Principles.

Formative conducts pre-engagement and ongoing vendor assessments to ensure that proper data privacy and security practices are in place throughout the vendor relationship.

Changes to existing contracts or to vendor services require a security-risk assessment in order to confirm that the changes do not present additional or undue risks.

DATA BREACH NOTIFICATION

If Formative learns of a data breach, we will follow our Incident Response Plan and notify our customers without undue delay.

POLICY & PROCEDURE DOCUMENTS ALIGN WITH NIST CSF, SOC 2, GDPR, & ISO

Formative reviews its systems against applicable state, federal, and internal regulations as well as against controls associated with NIST CSF, SOC2, GDPR, and ISO. Formative accordingly addresses any identified risks or gaps.

We have a designated Privacy and Compliance Committee that holds quarterly meetings in order to ensure data integrity.

POLICIES & STANDARDS

Formative maintains comprehensive policies and standards for information security and data protection that take into consideration data-privacy laws and regulations, including data-retention requirements, that are applicable to jurisdictions in which Formative operates.

The Privacy and Compliance Committee reviews and approves these policies and standards. Formative annually reviews its Global Privacy and Compliance Program, and we review other policies and standards at least every three years in accordance with company policy.

Formative's Privacy and Compliance Committee, which consists of representatives from various business units, maintains the process to develop, review, update, and decommission information security alongside privacy policies and standards. Additionally, changes in the risk environment or regulatory landscape may also trigger reviews.

Formative aligns its policies and standards to all applicable state, federal, and international privacy laws as well as with recognized industry standards, including (but not limited to) the following:

- U.S. Sentencing Guidelines: Seven Elements of an Effective Compliance Program
- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- General Data Protection Regulation (GDPR)
- ISO 27001
- System and Organization Controls (SOC 2).

Formative makes its policies and standards available to all personnel. These materials cover every aspect of the Information Security and Privacy Program, including the following:

- Identity and Access Management: for example, entitlement management and production access
- Application and Software Security: for example, software-change management, backup, and restoration
- Infrastructure Security: for example, capacity management, vulnerability management, and network & wireless security
- Mobile Security: for example, Bring Your Own Device (BYOD) and mobile applications
- Data Security: for example, cryptography, encryption, database security, data erasure, and media disposal
- Cloud Computing: for example, governance & security of cloud applications as well as Software-as-a-Service data onboarding
- Working-from-Home Best Practices: for example, safe data handling, clean desk guidelines, social engineering, and phishing awareness

Technical Safeguards

DATA ENCRYPTION

Data is encrypted in transit and at rest.

DATA RETENTION & DELETION

Formative has implemented a Data Retention Policy. Where appropriate, our solutions utilize automated rules to purge data according to this policy.

DATA BACKUP & BUSINESS CONTINUITY

We perform regular backups of data and systems. Backup intervals depend on the type of data, and they range from minutes to once per day.

Formative has a documented Business Continuity Plan, recovery procedures, and a trained response team. At a minimum, Formative tests the Business Continuity Plan and recovery procedures twice annually and incorporates any improvements into the Plan.

As an engineering principle, Formative applies redundancies, including self-healing features built into the platform that automatically adjust to outages wherever possible.

VULNERABILITY REMEDIATION

Formative has a Vulnerability Remediation policy to identify and remediate vulnerabilities according to the risk they present. We utilize monitoring and management software in order to monitor systems and to ensure that patches are implemented.

MALWARE PROTECTION

Formative has anti-malware and anti-spam solutions in place to protect servers and workstations.

LOGGING & MONITORING

Formative uses logging and monitoring solutions to identify and investigate possible security events.

IDENTITY & ACCESS CONTROL

Through login credentials, Formative limits access to personal information to only those employees who require such information in order to perform their job functions. Furthermore, Formative uses access controls such as Multi-Factor Authentication, Single Sign-On, least privilege & access on an as-needed basis, strong password controls, and restricted access to administrative accounts.

INFORMATION SECURITY & PRIVACY

Formative maintains an Information Security and Privacy Program which, along with security personnel embedded in each of our business units, consists of a centralized group that establishes information security mandates, evaluates adherence to these mandates, and detects & responds to incidents. Formative frequently adjusts this program to ensure ongoing suitability.

The Information Security and Privacy Program regularly assesses the sufficiency of Formative's controls. Additionally, the Program coordinates quarterly assessments of control efficacy and heightened residual risks through the IT Security and Privacy program.

Formative's Data Protection Officer (DPO) is responsible for managing and implementing the Information Security and Privacy Program and reports directly to the CFO (with dotted lines to our CEO and COO). The DPO's responsibilities include setting organization-wide control requirements, assessing adherence to controls, identifying & prioritizing data-privacy risks, and detecting & responding to incidents. The DPO reports the overall status of the information security and privacy program at quarterly intervals to the Privacy and Compliance Committee.

PENETRATION TESTS

No less than twice a year, Formative employs external firms to perform regular penetration testing.

NETWORK & COMMUNICATIONS

Formative hardens all network services and firewalls and employs continuous compliance monitoring that checks for changes to our standard configurations.

We use segregation principles at multiple levels for security, redundancy, and performance. Formative also requires NDAs from all parties that have or may have access to sensitive information resources.

SAAS ARCHITECTURE

Formative follows best practices for its system deployment and maintenance and for data maintained within AWS data centers and cloud services. We replicate and back up critical data and systems to secondary data centers. Formative has securely designed these systems, and the security & development teams review them before we put our systems into production.

COOKIE MANAGEMENT

Although Formative uses cookies to operate our sites, we have deployed a robust, best-in-class, cookie-management tool for all visitors and clients, a tool that allows each individual complete control of their personal data.

Risk Management

OUR APPROACH TO RISK MANAGEMENT

In order to provide appropriate risk governance, Formative employs a three-lines-of-defense model that offers accountability, oversight, and assurance. This model organizes risk-management activities across Formative's business units that own and manage risk (first line), perform independent-risk oversight functions (second line), and conduct an external audit (third line).

Within the first line, Formative's Privacy and Compliance Program establishes information security, outlines privacy standards, and sets clear expectations for Formative's adherence to these standards. Each business unit must understand any applicable controls and then abide by them. The Privacy and Compliance Committee functions as the second line and has oversight over the auditing of Formative's business-unit activities. Finally, Formative's External Audit acts as the third line, and it independently evaluates the company's control environment.

CERTIFICATIONS & AUDITS

Formative is proud to maintain a SOC 2 certification; in addition, reputable external auditing agencies audit us annually on our security standards.

Formative is currently GDPR-compliant and will be ISO 27001-certified and NIST CSF-compliant by the end of 2022.

We also perform regular internal audits to assess Formative's overall control environment; raise awareness of risks; communicate and report on the effectiveness of Formative's governance, risk management, and controls that mitigate current and evolving risks; and monitor the implementation of Management's control measures. Internal Audit is an independent function that reports to the Privacy and Compliance Committee.

Our customers also regularly audit Formative. We respond to these audits seriously, and we value the feedback from our customers.