Albany-Schoharie-Schenectady-Saratoga BOCES (Capital Region BOCES), in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.

- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;

- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);

- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov/data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, (518) 464-5139, DPO@neric.org, Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.

- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

- In the event that BOCES engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, (518)-464-5139, DPO@neric.org, 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on BOCES' website https://www.capitalregionboces.org/.

BY Vendor:

Alex Saltzman
Signature

Senior VP, Inside Sales
Title

10/13/2020
Date

EBSCO Information Services

Information Security Practices

White Paper

EBSCO Information Services
Information Security Practices

Revision Date: April 2020

Introduction

Information Security (IS) is a priority at EBSCO Information Services (EBSCO). Our mission is to incorporate security and risk management practices into our policies, procedures, and day-to-day operations within the organization. This approach enables appropriate diligence to ensure adequate protection of information assets and systems.

EBSCO's IS practices and strategies provide controls at multiple levels of the data lifecycle, from receipt to access, transfer, and destruction.

EBSCO is an international corporation producing products and services for customers across multiple markets. Our approach and tools will accommodate variances in requirements based on market or locale. We are committed to the confidentiality, integrity and availability of our information assets.

Information Security Policies & Management

EBSCO's Information Security Policy stands as the core of our IS program. Policies address security-related topics across the information asset lifecycle: from general policy roles – outsourcing security controls, change management, data classification, data retention and disposal, paper and electronic media, and system configuration requirements – to more specialized policies addressing anti-virus, encryption, backup, logging, and physical security controls. Our policies are developed in conjunction with the EBSCO Chief Information Officer (CIO) as well as the Legal, EBSCO Information Security and Business Continuity Management teams. The EBSCO IS office is responsible for maintaining all of EBSCO's information security policies, facilitating the development of processes for secure application development and security assessments, and auditing current practices to ensure compliance with policy.

EBSCO's Information Security team
The EBSCO IS team holds specific certifications (ISC2, SANS/GIAC) specializing in Information Systems, Intrusion Analysis / Prevention, Incident Handling, Computer Forensics, in addition to having years of experience working with industry security best practices.

IS is responsible for developing a strategy and approach to achieve objectives consistent with EBSCO's desired information security posture. EIS InfoSec is also responsible for developing, facilitating and/or overseeing the information policies, standards, guidelines, strategies and procedures; for conducting risk assessments; for managing incidents, and for providing internal / external reporting.

Lastly, IS constantly evaluates the effectiveness of ongoing security operational processes and monitors compliance for internal and external requirements. As such, a core component of our approach to protecting our information assets is continuous training and awareness of information security policies and procedures across all levels of personnel at EBSCO. As examples, EBSCO continues to mature its practices in the following areas:

- On-boarding education of EBSCO's information security policies and practices
- IS training and awareness based on roles and responsibilities, on handing and securing information assets
- Targeted information security discussion and presentations on security-related topics
- IS team access and membership to information security communities and organizations such as SANS, IAPP, BCI, DRI, etc.
- IS communications to EBSCO's employee population regarding latest threats, practices, guidelines, etc.

Information Asset Protection

EBSCO security policies provide a series of threat prevention and infrastructure management procedures, including the following:

Incident Management
EBSCO has an incident management approach that ensures security issues are handled accordingly. This involves ensuring incident response procedures are followed in order to contain or eradicate any threats or issues, taking due diligence in investigating and reporting the incident, taking appropriate steps to recover from the incident, and, if necessary, taking appropriate steps to escalate issues to senior management, law enforcement, or other key stakeholders. Events that directly impact customers are highest priority.

Post-event assessments are conducted to determine the root cause for events, regardless of threat, to understand if the causes are one-time, or trends, to adjust response or prevent recurrence.

Incident management procedures are exercised based on threat scenarios (e.g., insider threats, phishing, social engineering, software vulnerabilities) as needed to ensure that processes are efficient and stakeholders understand protocol.

Monitoring
EBSCO employs monitoring across its environments with multiple tools (a combination of open source and commercial tools) to identify, track, monitor, and report on pertinent risks, vulnerabilities (e.g., host availability, application response time, security events, etc.) Monitoring tools are set up to provide alarms and notices to EBSCO staff, who review and assess system logs to identify malicious activity.

Ongoing analysis across environments helps identify potential threats for escalation to EBSCO IS staff.

Vulnerability Management
The EBSCO IS team scans for security threats using commercial, automated and manual methods. The team is also responsible for tracking and following up on any potential vulnerabilities that might be detected. The team has the capability to scan environments (both internal and external) and is updated on new systems within our environment.

Once EBSCO's Technology and IS teams have identified a vulnerability, it is prioritized according to severity and impact and remediated accordingly. The EBSCO IS team tracks risk and vulnerabilities until remediation.

Malware Prevention, Detection & Remediation
EBSCO uses multiple tools to address malware and phishing risks (e.g., firewalls, anti-virus, backups, automated and manual scanning, end-user awareness). EBSCO's IS team periodically evaluates new technologies to mitigate malware and Advance Persistent Threats (APTs) to stay as protected as possible from these risks.

Network Security
EBSCO employs multiple layers of defense to secure information under our control, including protecting the network perimeter from external attacks – allowing only authorized services and protocols to access EBSCO's systems and services.

EBSCO's network security strategies, among other capabilities, include network segregation (e.g., production vs. testing, DMZ, service delivery vs. corporate).

Application Security
EBSCO employs Next Generation and Application Firewall technologies to mitigate the latest threat and attack vectors such as:

- Zero Day exploits
- Web application attacks (OWASP Top10)
- "Brute Force" and "Low and Slow" attacks
- Content scraping/harvesting
- Phishing/Spear Phishing
- Botnet/SpamBot activity
- Known malicious sources/actors

EBSCO leverages these technologies coupled with commercial threat intelligence feeds to create a comprehensive solution to detect and mitigate targeted application attacks before they have a chance for success.

Logical System Access
EBSCO has controls and practices to protect the security of customer information and employees. EBSCO maintains detailed logical access control security. Group access is used to grant employees access based upon their assigned function and job responsibility.

Each system user is assigned a unique user ID and password, and users are required to enter their current password prior to creating a new password.

Media Disposal
EBSCO utilizes a combination of internal processes and third-party vendors for media disposal. Destruction is based on the information asset classification and retention requirements. Certificates of destruction are collected, as required, from external third parties.

Logging Controls
EBSCO's policies provide that all event logs must be collected and protected from unauthorized access. The viewing of logs occurs only as required. The logs are further protected by a file integrity monitoring system that alerts the IS department of unauthorized access and modification.

Personnel Controls

EBSCO employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

EBSCO will verify an individual's education and previous employment, and perform internal and external reference checks. Where local laws or statutory regulations permit, EBSCO may also conduct criminal, credit, immigration, and security checks. The extent of background checks is dependent on the desired position.

Upon acceptance of employment at EBSCO, all employees are required to execute a confidentiality agreement that documents the receipt of, and compliance with, EBSCO policies.

At EBSCO, all employees are responsible for information security. As part of this responsibility, they are tasked with communicating security and privacy issues to designated management in Technology, IS, and/or the CIO.

Physical and Environmental Security

EBSCO has policies, procedures, and infrastructure to handle both the physical security of its data centers as well as the environment in which the data centers operate. These include:

Physical Security Controls

EBSCO's data centers employ a variety of physical security measures. The technology and security mechanisms used in these facilities may vary depending on local conditions such as building location and regional risks. The standard physical security controls implemented at EBSCO data centers includes the following:

- electronic card access control systems
- intrusion detectors and alarms
- computer inventory control
- interior and exterior cameras
- 24/7 security guard access

Access to areas where systems, or system components, are installed or stored is segregated from general office and public areas such as lobbies. The cameras and alarms for each of these areas are centrally monitored. Activity records and camera footage are kept for later review, as needed.

Access to all data center facilities is restricted to authorized EBSCO employees, approved visitors, and approved third parties whose job it is to operate the data center. EBSCO maintains a visitor access policy and procedures on approvals for visitors, third parties, and employees who do not normally have access to data center facilities. EBSCO audits who has access to its data centers on a regular basis.

EBSCO restricts access to its data centers based on role.

Environmental Controls

- **Power and Utilities –** EBSCO data centers have redundant electrical power which includes backup generators as well as multiple utility providers, services, and systems. Alternate power supplies provide power until diesel engine backup generators engage and are capable of providing emergency electrical power, at full capacity, as needed, and the redundancy of our multiple oil providers, geographically diverse, allows for continuous operation, if needed.

- **Climate Control –** EBSCO maintains redundant cooling systems to control our data center environments.

- **Fire detection, protection and suppression –** EBSCO fire protection systems include fire alarms, automatic fire detection, and fire suppression systems. Should a fire arise in our data centers, visible and audible alerts are activated and proper response is initiated, which include automated response as well as the use of physical fire extinguishers located throughout our data centers.

Scott Macdonald,
VP of Information Security and Operations

8 NYCRR Part 121	
121.2 Each educational agency shall ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with Federal and State law and the educational agency's data security and privacy policy.	BOCES Obligation
121.3(b) The bill of rights shall also be included with every contract an educational agency enters with a third-party contractor that receives personally identifiable information. The supplemental information must be developed by the educational agency and include the following Information:	BOCES Obligation
121.3(b)(1) What is the the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?	EBSCO will process personal data only: • where we need the Personal Information to perform a contract with you or your organization; • where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms; or • where we have your consent to do so. In some cases, we may also have a legal obligation to collect Personal Information from you or may otherwise need the Personal Information to protect your vital interests or those of another person. If we collect and use your Personal Information in reliance on our legitimate interests (or those of any third party), we will make clear to you at the relevant time what those legitimate interests are.
121.3(b)(2)Will the organization use subcontractors? If so, how will the organization ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., FERPA; *Education Law section 2-d*)?	No
121.3(b)(3)	7/1/2020 - ongoing

What is the duration of the contract including the contract's expected commencement and expiration date? Describe what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).	Upon contract termination, the library may request any data that has been provided to EBSCO as part of the contracted services be returned. Customer data will be removed from EBSCO's systems at the end of the contract period upon request and EBSCO will provide a written attestation of data destruction.
121.3(b)(4) how can a parent, student, eligible student, teacher or principal challenge the accuracy of the student data or teacher or principal data that is collected;?	Please see EBSCO's Privacy Policy for a complete description of how to exercise rights: https://www.ebsco.com/company/privacy-policy#prod_how-can-i-excercise-rights
121.3(b)(5) Describe where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.	EBSCO stores data in its greater Boston, MA USA data centers. EBSCO implements an extensive information security policy which focuses on web application security (to identify potential or realized weaknesses as a result of inadvertent misconfiguration, authentication, application logic, error handling, sensitive information leakage, etc.). This policy includes firewall and router security, data classification and control, vulnerability identification, authentication, encryption, etc. Further, EBSCO's data centers employ a variety of physical security measures. The technology and security mechanisms used in these facilities may vary depending on local conditions such as building location and regional risks. The standard physical security controls implemented at EBSCO data centers includes the following: • electronic card access control systems • intrusion detectors and alarms • computer inventory control • interior and exterior cameras • 24/7 security guard access
(6)address how the data will be protected using encryption while in motion and at rest.	All sensitive data is securely encrypted in the database with restricted access using AES-256. No sensitive data is stored in non-production environments.

	EBSCO provides encryption for data in transit with SS/TLS1.2 2048-bit encryption.
121.6(a)Please submit the organization's data security and privacy plan that is accepted by the educational agency.	Please see the attached **Information Security Whitepaper_EBSCO.**
121.6(a)(1) **Describe how the organization** will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;	EBSCO's information security and infrastructure teams focus on the confidentiality, integrity and availability of its information and systems. This approach uses a multitude of monitoring tools, processes and procedures to control access (user authentication and logical access controls); protect and prevent intrusions (antivirus software, firewalls, etc.); and identify, track, monitor, and report on pertinent security events. The information security incident management approach addresses any significant event, which includes communicating to all relevant individuals/groups within EBSCO for identification, categorization, analysis, remediation and monitoring. Please see the attached **Information Security Whitepaper_EBSCO** for additional information**.**
121.6(a)(2)specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;	EBSCO implements an extensive information security policy which focuses on web application security (to identify potential or realized weaknesses as a result of inadvertent misconfiguration, authentication, application logic, error handling, sensitive information leakage, etc.). This policy includes firewall and router security, data classification and control, vulnerability identification, authentication, encryption, etc.
121.6(a)(3)demonstrate that the organization complies with the requirements of section 121.3(c) of this Part	Please see EBSCO's Privacy Policy for details about user rights to data collected: https://www.ebsco.com/company/privacy-policy
121.6(a)(4)specify how officers or employees of the organization and its assignees who have access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access;	A core component of EBSCO's approach to protecting its information assets is continuous training and awareness of information security policies and procedures across all levels of personnel at EBSCO. As examples, EBSCO continues to mature its practices in the following areas:

	• On-boarding education of EBSCO’s information security policies and practices • Information Security training and awareness based on roles and responsibilities, on handling and securing information assets • Targeted information security discussion and presentations on security-related topics • Information Security team access and membership to information security communities and organizations such as SANS, IAPP, BCI, DRI, etc. • Information Security communications to EBSCO’s employee population regarding latest threats, practices, guidelines, etc. Please note that, EBSCO does not have the ability or bandwidth to train all individuals on privacy laws for each individual state. We have a comprehensive training program that covers requirements generally applicable to all states, education related laws such as FERPA and COPPA and GDPR for the EU.
121.6(a)(5)specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;	N/A
121.6(a)(6)specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;	EBSCO has an incident management approach that ensures security issues are handled accordingly. This involves ensuring incident response procedures are followed in order to contain or eradicate any threats or issues, taking due diligence in investigating and reporting the incident, taking appropriate steps to recover from the incident, and, if necessary, taking appropriate steps to escalate issues to senior management, law enforcement, or other key stakeholders. Events that directly impact customers are highest priority. Post-event assessments are conducted to determine the root cause for events, regardless of threat, to understand if the causes are one-time, or trends, to adjust response or prevent recurrence.

121.6(a)(7)describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.	At the end of the contract, any data EBSCO receives from the customer for use with the services (e.g., catalog data for use with *EBSCO Discovery Service*) will be returned to the customer upon request in the original format provided.
121.9(a) In addition to all other requirements for third-party contractors set forth in this Part, each third-party contractor that will receive student data or teacher or principal data shall:	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.
121.9(a)(1) describe the organization's adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework;	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.
121.9(a)(2)Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts; *Education Law section 2-d*; and this Part;	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.
121.9(a)(3) Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.
121.9(a)(4)Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract;	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.
121.9(a)(5)Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student; **(i)**except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with State and Federal law, regulations and its contract with the educational agency; or **(ii)**unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.
121.9(a)(6)Describe how the organization will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.
121.9(a)(7) Describe how the organization will use encryption to protect personally identifiable	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.

information in its custody while in motion or at rest; and	
121.9(a)(8)Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.
121.9(a)(b) Describe how the organization will supervise its subcontractors to ensure that as subcontractors perform its contractual obligations, the subcontractor will conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure.	N/A. EBSCO will not user third parties to fulfill the obligations in the contract.
121.10(a) Describe how the organization shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.	EBSCO will notify customers affected by a security breach within 72 hours of discovery of the breach.
121.10(c) Affirmatively state that the organization will cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.	EBSCO agrees to cooperate with educational and law enforcement agencies when investigating unauthorized disclosure of PII.
121.10(f) Affirmatively state that where a breach or unauthorized release is attributed to the organization, the organization shall pay for or promptly reimburse the educational agency for the full cost of such notification.	EBSCO will assume all costs associated with data breaches attributed to the organization.