EBSCO

EIS Information Security and Privacy Management System

A Publication of EBSCO Information Services (EIS)

March 2025

Table of Contents

Introduction

EBSCO Information Services (EBSCO) is the largest division of EBSCO Industries, a large, privately held corporation headquartered in Birmingham, AL, USA. EBSCO has diverse global operations and operates as a wholly owned subsidiary. While many aspects of EBSCO are operated independently, its Technology organization works in conjunction with the parent organization to gain leverage and economies of scale. EIS employs teams of highly experienced Information Security and Compliance professionals. EIS's Information Security team members are Subject Matter Experts in several areas including but not limited to: Information Security and Privacy, Regulatory Standards, Security Operations Engineering, Identity and Access Management Engineering, Agile product training and development and Cloud Architecture and Design.

EBSCO's researcher products, including EBSCOHost, EBSCO Discovery Services, Dynamed, Marketplace and CINHAL are primarily hosted in AWS US East Region 1, which is located in the greater Northern Virginia region. For FOLIO, Locate, OpenRS and Panorama hosting, EBSCO has hosting options across multiple AWS regions and will host data in the AWS region of the customer's choosing. GOBI is hosted in an on-premise data center in Contoocook, NH, USA, with our new MOSAIC book ordering platform hosted in AWS US East Region-1. EBSCONet is hosted within EBSCO Industries' data center in Birmingham, AL, USA, with migration to Amazon Web Services planned. EBSCOLearning, which includes LearningExpress and Accel, is hosted in AWS US East Region 1 and US West Region 2 in Oregon.

Applicability

This whitepaper is applicable to the following services:

- Administration and Configuration Services (EBSCOadmin, EBSCO Experience Manager, EBSCO Configuration Manager, IAM)
- Library Website Creation Services (STACKS)
- Library Management Systems (FOLIO, LOCATE, OpenRS)
- Panorama
- Library Aware
- EBSCONet, EBSCO Marketplace
- GOBI Library Solutions
- Discovery and Research Database Services (EBSCO Discovery Service (EDS), EBSCOhost, EBSCO Host Mobile, EDS API)
- Journals & e-Package Services (Global Knowledgebase, EBSCO Publishing Knowledgebase)
- Holdings Linking Services (Holdings Manager, Full Text Finder, Publication Finder, HoldingsIQ, LinkIQ, and Usage Consolidation)
- Electronic Resources Management (Flipster, eBooks, EBSCOhost Collection Manager ECM)
- EBSCOLearning (LearningExpress, Accel)
- EBSCO Health (CINAHL, Patient Education Reference Center, Nursing Reference Center, Nursing Reference Center Plus, Continuing Medical Education (CME))
- Health Knowledge Products (Dynamed, Dynamic Health, Dynamedex, Dyna AI)

  Dynamed Decisions, MyHealth Decisions

Information Security and Privacy Policy

EBSCO has implemented an Information Security and Privacy Management System (ISPMS) in line with the International Standards for Information Security and Privacy, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO/IEC 27701. These standards define the requirements for an ISPMS based on internationally recognized best practices.

These policies apply to systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to EIS systems. It is a fundamental principle of the EIS's Information Security and Privacy Management System that the controls implemented are driven by business needs and is regularly communicated to all staff through team meetings and briefing documents.

The operation of the ISPMS has many benefits for the business, including:

- Protection of Customer and Patron data
- Ensuring the supply of goods and services to customers
- Compliance with legal and regulatory requirements

EBSCO maintains certification to ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017, and ISO/IEC 27018 to ensure effective adoption of information security and privacy best practices. This program is validated by an independent Registered Certification Body (RCB) third-party auditing organization, external to EIS. The externally hosted certificate (#1737791-6) can be found here.

A clear definition of the requirements for information security within EIS is enforced and maintained with the internal business processes and external customers alike so that all information security and privacy program activity is focused on the fulfilment of those requirements. Statutory, regulatory and contractual requirements are also documented and incorporated into product planning processes. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

EBSCO's privacy policy can be found here

Access Control

The control of access to EBSCO's information assets is a fundamental part of a defense-in- depth strategy for information security. EIS's information security team works to protect the confidentiality, integrity, and availability of classified data by ensuring that a comprehensive mix of physical and logical controls are in place.

EIS's access control policy is designed to take account of the business and information security requirements of the organization and is subject to regular review to ensure that it remains appropriate.

The concept of Least Privilege Access is adhered to throughout EIS's access controls. EBSCO's information security team works to ensure that this concept is adhered to throughout EBSCO's information systems. Two-factor authentication is in place for EIS employee access, as well as industry standard password parameters which incorporate minimum password length, complexity requirements, password rotations, automatic lockout, etc.

EBSCO has a dedicated identity and access management team that works with the organization to provide a segregation of duties between access provisioning and system management. We adhere to a comprehensive access approval process for privileged access.

Artificial Intelligence Security

At EBSCO, we are committed to upholding the principles of responsible research as our guiding framework for working with AI.

EBSCO recognizes the importance of trust and aims to develop AI technologies that enhance, rather than replace, human expertise in the research process. Committed to responsible AI development, our processes and technologies are grounded in authoritative data and ensuring content accuracy.

A key aspect of EBSCO's AI philosophy is transparency. We are committed to clear labeling of AI-generated content and providing explainable AI features. This allows users to understand how systems arrives at results, fostering informed decision-making and responsible use of the technology. EBSCO believes that by prioritizing transparency and explainability, we can empower users to critically evaluate and effectively utilize AI tools in their research endeavors.

Essentially, EBSCO aims to be a leader in responsible AI development within the research sector. By adhering to globally respected research practices and prioritizing accuracy, transparency, and human oversight, we are working to ensure that AI serves as a valuable tool for researchers, ultimately advancing the pursuit of knowledge and discovery.

Asset Management

EBSCO maintains a current, accurate inventory of assets associated with all information processing facilities. EIS has a comprehensive data catalog that identifies risks within the organization, These activities are coordinated by members of the Information Security, and Governance, Risk and Compliance (GRC) teams. EBSCO works to ensure that all legal and regulatory requirements are adhered to when considering the sensitivity of data.

EBSCO also maintains a comprehensive inventory of all physical assets, such as workstations and servers providing customer services. EIS works to ensure that all information security requirements are adhered to throughout a physical asset’s lifespan.

Availability Management

EIS strives to ensure high availability environments for our customers in on-premise data centers and in the AWS Cloud environment. Current status of EBSCO services can be found here.

Requirements for the availability of information processing facilities are established in conjunction with system owners and other interested parties to be equal to or better than the following:

- Services are designed to have all page loads delivered to the user in an average time of 5 seconds or less.
- End-to-end availability of the services (Customer SLA expectations are 99.9% uptime which is equal to less than 9 hours total downtime per year)
- Restore Time Objective maximum is 10 minutes for critical systems, meaning that systems shall be brought up within 10 minutes after an incident affects uptime.

- Minimum Restore Point Objective is 8 hours for critical systems, meaning critical systems shall be backed up at least once every 8 hours allowing data in the event of a data restore to be no more than 8 hours old.

Care is taken to ensure that such availability and reliability targets are measurable and understood across the organization. Procedures and tools are implemented to record the availability of all key services for which targets are specified. Availability statistics are published as part of the management reporting cycle and reflect the availability targets discussed above.

Procedures and tools are implemented to record the actual availability of key services for which targets are specified. Mechanism of calculating availability of end-to-end measurements are transparent so that a common understanding of how figures are arrived at is reached.

EBSCO or our Service Providers will also monitor the availability of key components that support the services provided so that data is available for analysis when investigating the causes of service outages.

Availability statistics are published as part of the management reporting cycle and will refer to the targets agreed. Where a target has not been met, some indication of the reason and actions that are to be taken will be provided. Please refer to status.ebsco.com for information on uptime. From there, Customers can sign up to be notified in the event of an outage.

Planned unavailability will be communicated to all Customers. In the event of a service needing to be withdrawn because of an incident, EBSCO or our Service Provider will make all reasonable endeavors to keep Customers and Patrons informed of the status and likely service restoration timelines.

All change requests will be assessed for implications to availability of products and services as part of a robust set of change management processes. Internal Teams work to ensure that availability mentioned in this policy is maintained as changes are implemented within production environments.

Backup Plan

EBSCO works diligently to ensure sufficient contingency resources and plans are implemented and tested regularly. This is achieved by deploying resources across multiple on-premise data centers and their virtual equivalents in AWS Availability Zones (AZ). This diversified approach to resource hosting ensures redundancy and fault tolerance, minimizing the impact of potential disruptions. To safeguard Customer data and ensure business continuity, we implement a robust backup and recovery strategy.

To streamline and automate backup processes, robust technologies are used for AWS and on-premise assets. Thess services manage and schedule backups for our physical compute and AWS resources, such as EC2 instances, EBS volumes, and RDS databases.

Our recovery strategy is designed to minimize downtime and data loss for our customers. We have defined clear Recovery Time Objective (RTO) and Recovery Point Objective

(RPO) metrics to guide recovery procedures. We also maintain a "pilot light" (hot standby) environment in separate regions and Availability Zones, allowing us to quickly redirect traffic and scale up in case of a major disruption.

Our comprehensive disaster recovery plan is well-documented, outlining step-by-step procedures for restoring data and applications. Regular testing ensures that our recovery processes meet our defined RTO and RPO targets. Furthermore, we continuously monitor our systems and have alerting mechanisms in place to proactively detect and respond to potential issues.

A central EBSCO philosophy is to avoid disruptive events by designing redundancy and resiliency into all operations. We do this by establishing geographically and technically diverse and redundant facilities and conduct regularly test backup failover scenarios. Tests are completed at a minimum once per year. No customer involvement is required to manage backups.

Business Continuity Plan

EBSCO Business Continuity plans are integrated and interdependent. They are oriented towards simple action plans that guide management and staff to the appropriate response during business disrupting events by ensuring effective communications, efficiency, and execution in mind. EIS success relies on the sustainability of these efforts. As such, we strive to embed business continuity principles and practices across the organization in standard operating procedures.

The Business Continuity Plan establishes EBSCO's strategy for the management of resources and maintaining operations in the event of a disaster or potential disruption in services. The Business Continuity Plan is approved by Senior Management and is reviewed annually and upon significant change across the environment.

EBSCO performs multiple tests per year of our various systems and plans that are part of the overall approach to Business Continuity. EIS's culture of continuous improvement facilitates action based on results of each test.

EBSCO has successfully demonstrated the resilience of this program through severe emergencies, including floods, tornadoes, hurricanes and local facility disruptions. Our preparations have allowed us to continue operating the business and delivering services without impacting our customers. While proud of this fact, we remain diligent in ensuring our products will continue to deliver services to our customers, regardless of whatever extraordinary events may occur. EIS has embraced cloud-based tools throughout the enterprise and leverages remote workforce capabilities extensively.

Cryptography

EBSCO products use HTTPS and TLS 1.2/1.3 to protect the transmission of data from users to our systems. Within our systems, sensitive customer data is protected using AES 256 encryption by default.

EBSCO Information Security establishes requirements for the use of encryption techniques through the implementation of this policy. It's employed for the protection of

sensitive data at rest, in transit, in use, or required by contract. The controls and related procedures for the various areas where encryption and other cryptographic techniques are required by Federal and International law and are FIPS 140-2 compliant.

No customer involvement is required for the encryption of data within the EBSCO platform.

Customer Control Responsibilities

Customers of EBSCO, in consultation or assistance with our support team, are responsible for configuring authentication to our services. They are also responsible for notifying EBSCO of settings, or configurating access to services via Single Sign On to ensure that access to EBSCO databases are removed when a user leaves the applicable institution. EBSCO is responsible for the rest of security controls within our platform.

No customer action is required to ensure clock synchronization within our platform.

For more information on EBSCO's authentication options please refer to here.

https://www.ebsco.com/sites/g/files/nabnos191/files/acquiadam-assets/Authentication-Solutions-Guide.pdf

Human Resource Security

Appropriate background verification checks are carried out on all employees prior to hire. Employment contracts, including those with contract staff, specify relevant requirements for information security and privacy, including a commitment to comply with EIS policies. This includes comprehensive acceptable use and confidentiality agreements which all employees must acknowledge.

All employees with access to EIS systems are required to take twice annual security and privacy awareness training. Role-based training is required for certain employees and contractors to an appropriate level of detail.

Incident Response

EIS's incident response plan (IRP) defines procedures to be followed and appropriate level actions to be taken during different phases of an incident response, should one occur. The plan defines these phases, the appropriate corresponding response and approach to collecting and implementing lessons learned. The plan supports the level of resource availability our customers both require and expect.

EIS's IRP includes procedures to limit the impact of any security incident and provides for the required customer and internal communications detailing the incident. EIS is committed to making sure all reporting, legal and regulatory requirements are met.

Stakeholders throughout the organization, including security operations, governance risk and compliance, the CIO office, senior management have roles defined within the EIS

IRP. Incidents are handled via a defined process, with common scenarios mapped out for teams ahead of time. Incidents are followed up with lessons learned, with incident response plans and runbooks updated as a result of these lessons learned.

Were a breach to occur, EBSCO will notify customers within 72 hours of any confirmed breach of customer data. Where applicable, EBSCO will comply with applicable laws regarding the notification to public authorities or the public in the event of a breach.

If customer's suspect misuse of the EBSCO platform, please contact eis_compliance@ebsco.com.

Logging and Monitoring

EBSCO has a Security Operations team that handles logging and monitoring for our internal environment. This includes all products within our scope and boundaries. At this time we do not offer integration with customer security logging systems.

EBSCO employs a 24/7 SOC (Security Operations Center) managed within a Security Incident Event Monitoring system. Our talented security operations team, in conjunction with an external SIEM provider and automated assistance, reviews alerts for abnormalities within our systems.

The EIS Logging and Monitoring Policy outlines procedures for setting up and managing internal logs to monitor system usage, ensuring the security and integrity of EIS and Customer information assets. It applies to all individuals and systems within EIS, including employees, suppliers, and third parties with system access.

EBSCOThe policy mandates the activation of audit logging facilities on all relevant equipment to record key events, access attempts, and system changes. It also requires regular review of audit logs based on factors like business criticality and information sensitivity. The policy emphasizes the protection of log information through strict permissions, archiving, and daily backups.

Additionally, EBSCO address's fault logging, requiring an investigation of reported faults to ensure security control integrity. We also ensure the synchronization of system clocks for accurate incident investigation and logging of administrator activities.

Media Sanitization and Disposal

EBSCO has established guidelines for secure sanitization and destruction methods used to protect against the unauthorized disclosure of sensitive information in the process of reallocating or disposing of media.

In addition, many EIS products and services are hosted via Amazon Web Services, which adheres to multiple security and privacy frameworks and associated requirements for proper disposal of media. All media awaiting sanitization or disposal shall be handled and stored as if it contains "confidential information" in accordance with current policy guidelines. Media shall be sanitized or destroyed only by EBSCO IT support personnel, Information Security, or a licensed secure disposal vendor.

Media sanitization or destruction activities are recorded to include the following minimum information and be retained for at least 1 year.

- Description of media
- Date media was sanitized or destroyed
- Name of individual or vendor who performed the media sanitization/destruction
- Method of sanitization/destruction used
- Hard drives are first degaussed, then shredded, then crushed.

Contracts and service agreements with vendors include accommodations for EIS to sanitize, destroy, encrypt, or otherwise retain removable media prior to returning equipment to the vendor for any reason.

Network Security

EBSCO's network security design includes a Defense-in-Depth approach with multiple layers of controls.

These controls consist of but are not limited to:

- Default Deny rules on Edge Routers
- Default Deny Rulesets on Firewalls
- Segmented Architectures (Application, Presentation, Session and Back-end Layers)
- Web Application Firewalls are used at appropriate segmented layers

Physical Security

EBSCO is committed to ensuring the safety of its employees, contractors and assets and takes the issue of physical security very seriously. EIS has a comprehensive set of physical security controls which ensure that its data centers and offices are sufficiently protected. Access to data centers and offices is limited only to necessary personnel, and all access is logged and reviewed for abnormalities.

EBSCO also contracts with Amazon Web Services (AWS) to provide world class security within their hosted data centers. For more information on physical security in AWS hosted environments see here.

Privacy Considerations

EBSCO has built an environment which is compliant with all major privacy regulations. This includes but is not limited to, GDPR, UK Data Protection Act, CCPA, CPRA, FERPA, COPPA, HIPAA, Virginia CPDA, Canadian PIPEDA, Australian Privacy Act, Brazil General Data Protection Law, Connecticut CTDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Protection of Personal Information Act (South Africa). EBSCO's Governance Risk and Compliance team regularly reviews new privacy laws as

they are implemented in order to ensure that our products comply with privacy laws and regulations where our products are stored.

EBSCO is a processor of information that is provided directly from customers, or information within the EBSCO's FOLIO Hosting product.

EBSCO allows the option for users to create user accounts in order to personalize their research experience with EBSCO. In this case, EBSCO acts as a joint controller of this information. This means that EBSCO has implemented application functionality to enable Patron Users to exercise their privacy rights, including but not limited to the right to view modify and delete their personal information, directly within their account self service module or by contacting privacy@ebsco.com. This requires no action by the Institutional Customer Administrator.

Privacy Considerations for EU Data Locality

EBSCO offers hosting options in the European Union for use with Folio, Locate and OpenRS to handle data residency requirements for our customers located in the European Union. For other products, information is hosted in the United States, however we do comply with GDPR and have attested to the EU/US Data Privacy Framework covering cross border transfers with a European Commission adequacy decision. In addition, our standard license agreement includes Standard Contractual Clauses, which cover cross border data transfers in the event that the EU/US Data Privacy framework is invalidated by European authorities.

For customers with residency requirements, EBSCO offers options to prevent personal data transferred to the United States. When creating a MyEBSCO account via single sign-on, the institution or library has control over what data are shared to EBSCO. The minimum requirement is a unique identifier (which can be a pseudonymous identifier), whereas first name, last name, and email address are optional.

In addition, for customers in Europe who purchase EBSCO's researcher tools (i.e., EBSCOHost and EBSCO Discovery Services), but do not subscribe to Folio/Locate, we offer integration with OpenAthens, an identity federation service hosted in the United Kingdom. In this case, we are able to offer the same pseudonymous identifiers for data which is transferred to the US.

Security Assertion Markup Language (SAML) Single Sign-On (SSO) can be configured to limit personal information shared during the authentication process. This ensures sensitive data remains within the Customer organization's IT boundaries while also enabling secure access to EBSCO SaaS applications. To achieve this, EBSCO products can be configured using SAML SSO Attribute Mapping and Filtering.

SAML SSO uses assertions to pass user attributes (e.g., name, email) to a Service Provider (SP) during authentication to EBSCO products and services. During the product implementation and configuration phase, such sensitive identifiers (e.g., real names) are replaced with opaque, organization-specific identifiers that are not considered sensitive by the Customer. In other cases, data elements can also simply be prevented from being passed to EBSCO. This can be accomplished with little to no loss of product functionality.

Secure Development

EBSCO has a comprehensive secure development program, with gated controls to ensure that all code is reviewed and tested to OWASP top forty vulnerabilities and other defects prior to migration to production. In addition, approval from appropriate personnel is required within our code deployment pipeline before code can be brought to production.

As part of the change management process, EBSCO requires development teams to assess the impact to privacy and security of major changes (such as a change in data collection)

Teleworking

Many EBSCO employees have the option to work remotely, also known as teleworking. As a result, EBSCO has implemented a complete set of controls to ensure the security of data for teleworking employees.

EBSCO's clear desk and clear screen policy applies to all our employees when working remotely. Additionally, EBSCO has controls to encrypt, and remotely wipe workstations which ensures the security of data in remote use workstations.

Remote access to EBSCO's internal network is protected through secure VPN which is authenticated via two factor authentication. Preventing unauthorized access to company data from insecure networks is of utmost importance to EBSCO. Upon termination for any reason all equipment supplied must be returned to EBSCO.

Vendor Management

Our relationships with suppliers are based on a clear understanding of our expectations and requirements around information security. These requirements are documented and clearly emphasize the importance placed on maintaining and continually evolving the effectiveness of implemented controls to reduce organizational risk and maintain informational security and privacy for our customers.

EBSCO's Vendor Due Diligence program is based on ISO/IEC 27001:2022 and ISO/IEC 27002:2022, targeting specific areas based on EIS's security requirements. EBSCO conducts Data Protection Impact Assessments on all vendors. EBSCO also has a due diligence questionnaire that is sent out to vendors where applicable. EBSCO's subprocessors hold SOC 2 Type 2 and/or ISO 27001 certifications, and these audit reports are regularly reviewed by EIS's compliance team to ensure that controls at subprocessors meet EIS's strict standards.