EBSCO

EIS Information Security and Privacy Management System

A Publication of EBSCO Information Services (EIS)

January 2023

Table of Contents

Introduction

EBSCO Information Services (EIS) is the largest division of EBSCO Industries, a large, privately held corporation headquartered in Birmingham, AL, USA. EIS has diverse global operations and operates as a wholly owned subsidiary. While many aspects of EIS are operated independently, its Technology organization works in conjunction with the parent organization to gain leverage and economies of scale. EIS employs 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 Compliance, Regulatory Standards, Security Operations Engineering, Identity and Access Management Engineering, Agile product training and development and Cloud Architecture and Design.

EIS employs a hybrid cloud model, between AWS US East Region 1 in the cloud, and legacy data centers in Ipswich, MA, USA and Boston, MA, USA for our EBSCOHost, EBSCO Discovery Services and DynaMed family of products. For FOLIO 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. Some backend services are supported by EBSCO Industries data center in Birmingham, AL, USA, however no customer databases are stored in the Birmingham Data Center. Accel5 is a customized version of the Thought Industries platform and is hosted in the Thought Industries AWS Instance.

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)
- Panorama
- Library Aware
- 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, Audiobooks, EBSCOhost Collection Manager ECM)
- eLearning Resources (LearningExpress, Accel5)
- EBSCO Health (CINAHL, Patient Education Reference Center, Nursing Reference Center, Nursing reference Center Plus)
- Health Knowledge Products (Dynamed, Dynamic Health)
- Dynamed Decisions, MyHealth Decisions

Information Security and Privacy Policy

EIS 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 all 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 user data

- Ensuring the supply of goods and services to customers
- Compliance with legal and regulatory requirements

EIS has decided to maintain certification to ISO/ IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB). The externally hosted certificate (#1737791-2) can be found here.

A clear definition of the requirements for information security within EIS will be agreed to and maintained with the internal business and customers so that all ISPMS activity is focused on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

Media Sanitization and Disposal

EIS 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 DOD and NIST requirements in their 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.

Asset Management

An inventory of assets associated with information processing facilities within EIS is maintained. EIS has a comprehensive data catalog that identifies risky assets within our organization, and the business intelligence team works regularly with the Governance,

Risk and Compliance team. EIS works to ensure that all legal and regulatory requirements are adhered to when considering the sensitivity of data.

In addition, EIS maintains a comprehensive inventory of all physical assets, such as workstations and servers, which are used to provision customer services. The GRC team works to ensure that all information security requirements are adhered to throughout a physical asset's lifespan.

Access Control

The control of access to our information assets is a fundamental part of a defense-in-depth strategy to 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. EIS's information security team works to ensure that this concept is adhered to throughout EIS'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.

Cryptography

To identify those areas in which the deployment of cryptographic techniques are required, EIS takes a managed risk-based approach. This approach includes but is not limited to; performing risk assessments, using acceptable encryption techniques, ensuring proper deployment into the environment, and PHI is appropriately protected. Additionally, custom software is reviewed and tested, and cryptographic key management is in place as outlined in NIST 800-57.

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

EIS 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.

Physical Security

EIS 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 is limited only to necessary personnel, and all access is logged and reviewed for abnormalities.

EIS also contracts with AWS for the processing of customer data, who provide world class security within their hosted data centers. For more information on physical security in AWS hosted environments see:
https://aws.amazon.com/ compliance/data-center/controls/.

Network Security

EIS'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 ACL list on Edge Routers
- Default Deny Rulesets on Firewalls
- Application, Presentation, Session and Backend Layers are segmented
- Web Application Firewalls are used throughout each segmented layer

Secure Development

EBSCO has a comprehensive secure development program, with gated controls to ensure that all code is reviewed and tested to OWASP top 40 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)

Vendor Management

Our relationships with suppliers are based on a clear understanding of our expectations and requirements around information security. These requirements are documented clearly emphasizing 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.

EIS's Vendor Due Diligence program is based on ISO/IEC 27001/2, 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.

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 details 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 will inform customers within one business day of any confirmed data beach and provide a timely incident analysis. EIS's legal team is committed to making sure all reporting, legal and regulatory requirements are met.

Were a breach to occur, EBSCO will notify customers within 72 hours of any confirmed breach of customer data. EBSCO will then provide the results of an investigation into the breach, as well as a summary of remediation efforts that have taken place. 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

Availability Management

EIS strives to ensure High Availability environments for our customers in legacy data centers and in the AWS Cloud environment.

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 (Majority of DDE Customer SLA expectations are 99.5% to 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 a disaster 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 less than 8 hours old.

Care is taken to ensure that the targets and their availability are agreed upon, measurable and if any additional tools are required to track performance against these targets, they will be subject to the approval of a business case. Procedures and tools will be put in place to record the actual availability of key services for which targets are specified. Availability statistics will be published as part of the management reporting cycle and will refer to the targets agreed.

Procedures and tools will be put in place to record the actual availability of key services for which targets are specified. Where these are end-to-end measurements, the mechanism of calculating availability will be agreed with the customer of the service so that a common understanding of how figures are arrived at is reached.

EIS 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 will be 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 given. Please refer to status.ebsco.com for information on downtime. From there customers can sign up to be notified in the event of downtime.

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

As part of the change management process, all change requests will be assessed for implications to availability of products and services. Teams shall work to ensure that availability mentioned in this policy will be maintained as changes are migrated to production.

Business Continuity Plan

EIS believes that business continuity plans need to be integrated and interdependent. They need to be orientated to the user in the form of simple action plans that guide management and staff to the appropriate response to a business disrupting event with effective communications, efficiency, and execution in mind. Additionally, we believe that our long-term success relies on the sustainability of these efforts. As such, we strive to have business continuity principles and practices embedded in standard operating procedures. There are times, though, when extraordinary events require special planning.

Examples of these include:

- Business Continuity Plan

- Incident Response Plan
- Backup Plans

The Business Continuity Plan establishes EIS'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.

EIS 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.

EIS has dealt with severe emergencies, including floods, tornadoes, hurricanes and local facility disruption. Our preparations have allowed us to continue conducting business, delivering services and operating without impacting our customers. While proud of this fact, we remain diligent in ensuring our services 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.

Backup Plan

A central philosophy of ours is to avoid crippling effects of events by designing redundancy and resiliency into our operations. We do this whenever economically feasible by establishing geographically and technically diverse and redundant facilities. Our legacy data centers operate in an "N+1 live" configuration. For example, we regularly bring data centers out of service (down) for maintenance with zero impact to customers or users of our systems.

As part of our cloud transformation process, EIS has implemented a hybrid model with Amazon Web Services, connected to our legacy data centers via AWS direct connect. Our AWS environment is built in multiple availability zones with redundancies implemented throughout or AWS instance. EBSCO regularly tests failover scenarios between availability zones. Tests are completed at a minimum once per year. No customer involvement is required to manage backups.

Human Resource Security

Prior to hire, 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, including a commitment to comply with EIS policies in this area and are required in certain countries. This includes comprehensive acceptable use and confidentiality agreements which all employees must adhere to. All employees with access to EIS systems are required to take annual security awareness training. Role based training is required for certain employees and contractors to an appropriate level of detail.

Teleworking

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

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

Remote access to EIS'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 EIS. Upon termination for any reason all equipment supplied must be returned to EIS.

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 will allow users to exercise their privacy rights, which includes but is 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 on the institutional administrator.

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, or configurating with Single Sign On so 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