EBSCO LICENSE AGREEMENT

By using the services available at this site or by making the services available to Authorized Users, the Authorized Users and the Licensee agree to comply with the following terms and conditions (the "Agreement"). For purposes of this Agreement, "EBSCO" is EBSCO Publishing, Inc.; the "Licensee" is the entity or institution that makes available databases and services offered by EBSCO; the "Sites" are the Internet websites offered or operated by Licensee from which Authorized Users can obtain access to EBSCO's Databases and Services; and the "Authorized User(s)" are employees, students, registered patrons, walk-in patrons, or other persons affiliated with Licensee or otherwise permitted to use Licensee's facilities and authorized by Licensee to access Databases or Services. "Authorized User(s)" do not include alumni of the Licensee. "Services" shall mean EBSCO*host*, EBSCO*host Integrated Search*, *EBSCO Discovery Service*, EBSCO eBooks, Flipster and related products to which Licensee has purchased access or a subscription. "Services" shall also include audiobooks and eBooks to which a Licensee has purchased access or a subscription and periodicals to which Licensee has purchased a subscription. "Databases" shall mean the products made available by EBSCO. EBSCO disclaims any liability for the accuracy, completeness or functionality of any material contained herein, referred to, or linked to. Publication of the servicing information in this content does not imply approval of the manufacturers of the products covered. EBSCO assumes no responsibility for errors or omissions nor any liability for damages from use of the information contained herein. Persons engaging in the procedures included herein do so entirely at their own risk.

I. LICENSE

A. EBSCO hereby grants to the Licensee a nontransferable and non-exclusive right to use the Databases and Services made available by EBSCO according to the terms and conditions of this Agreement. The Databases and Services made available to Authorized Users are the subject of copyright protection, and the original copyright owner (EBSCO or its licensors) retains the ownership of the Databases and Services and all portions thereof. EBSCO does not transfer any ownership, and the Licensee and Sites may not reproduce, distribute, display, modify, transfer or transmit, in any form, or by any means, any Database or Service or any portion thereof without the prior written consent of EBSCO, except as specifically authorized in this Agreement.

B. The Licensee is authorized to provide on-site access through the Sites to the Databases and Services to any Authorized User. The Licensee may not post passwords to the Databases or Services on any publicly indexed websites. The Licensee and Sites are authorized to provide remote access to the Databases and Services only to their patrons as long as security procedures are undertaken that will prevent remote access by institutions, employees at non-subscribing institutions or individuals, that are not parties to this Agreement who are not expressly and specifically granted access by EBSCO. For the avoidance of doubt, if Licensee provides remote access to individuals on a broader scale than was contemplated at the inception of this Agreement then EBSCO may hold the Licensee in breach and suspend access to the Database(s) or Services. **Remote access to the Databases or Services is permitted to patrons of subscribing institutions accessing from remote locations for personal, non-commercial use. However, remote access to the Databases or Services from non-subscribing institutions is not allowed if the purpose of the use is for commercial gain through cost reduction or avoidance for a non-subscribing institution.**

C. Licensee and Authorized Users agree to abide by the Copyright Act of 1976 as well as by any contractual restrictions, copyright restrictions, or other restrictions provided by publishers and specified in the Databases or Services. Pursuant to these terms and conditions, the Licensee and Authorized Users may download or print limited copies of citations, abstracts, full text or portions thereof, provided the information is used solely in

accordance with copyright law. Licensee and Authorized Users may not publish the information. Licensee and Authorized Users shall not use the Database or Services as a component of or the basis of any other publication prepared for sale and will neither duplicate nor alter the Databases or Services or any of the content therein in any manner, nor use same for sale or distribution. Licensee and Authorized Users may create printouts of materials retrieved through the Databases or Services online printing, offline printing, facsimile or electronic mail. All reproduction and distribution of such printouts, and all downloading and electronic storage of materials retrieved through the Databases or Services shall be for internal or personal use. Downloading all or parts of the Databases or Services in a systematic or regular manner so as to create a collection of materials comprising all or part of the Databases or Services is strictly prohibited whether or not such collection is in electronic or print form. Notwithstanding the above restrictions, this paragraph shall not restrict the use of the materials under the doctrine of "fair use" as defined under the laws of the United States. Publishers may impose their own conditions of use applicable only to their content. Such conditions of use shall be displayed on the computer screen displays associated with such content. The Licensee shall take all reasonable precautions to limit the usage of the Databases or Services to those specifically authorized by this Agreement.

D. Authorized Sites may be added or deleted from this Agreement as mutually agreed upon by EBSCO and Licensee

E. Licensee agrees to comply with the Copyright Act of 1976, and agrees to indemnify EBSCO against any actions by Licensee that are not consistent with the Copyright Act of 1976.

F. The computer software utilized via EBSCO's Databases and Service(s) is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this software, or any portion of it, is not allowed. User shall not reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the software, or create derivative works from the software.

G. The Databases are not intended to replace Licensee's existing subscriptions to content available in the Databases.

H. Licensee agrees not to include any advertising in the Databases or Services.

II. LIMITED WARRANTY AND LIMITATION OF LIABILITY

A. EBSCO and its licensors disclaim all warranties, express or implied, including, but not limited to, warranties of merchantability, noninfringement, or fitness for a particular purpose. Neither EBSCO nor its licensors assume or authorize any other person to assume for EBSCO or its licensors any other liability in connection with the licensing of the Databases or the Services under this Agreement and/or its use thereof by the Licensee and Sites or Authorized Users.

B. THE MAXIMUM LIABILITY OF EBSCO AND ITS LICENSORS, IF ANY, UNDER THIS AGREEMENT, OR ARISING OUT OF ANY CLAIM RELATED TO THE PRODUCTS, FOR DIRECT DAMAGES, WHETHER IN CONTRACT, TORT OR OTHERWISE SHALL BE LIMITED TO THE TOTAL AMOUNT OF FEES RECEIVED BY EBSCO FROM LICENSEE HEREUNDER UP TO THE TIME THE CAUSE OF ACTION GIVING RISE TO SUCH LIABILITY OCCURRED. IN NO EVENT SHALL EBSCO OR ITS LICENSORS BE LIABLE TO LICENSEE OR ANY AUTHORIZED USER FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES RELATED TO THE USE OF THE DATABASES OR SERVICES OR TO THESE TERMS AND CONDITIONS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

C. Licensee is responsible for maintaining a valid license to the third party resources configured to be used via the Services (if applicable). EBSCO disclaims any responsibility or liability for a Licensee accessing the third party resources without proper authorization.

D. EBSCO is not responsible if the third party resources accessible via the Services fail to operate properly or if the third party resources accessible via the Services cause issues for the Licensee. While EBSCO will make best efforts to help troubleshoot problems, Licensee acknowledges that certain aspects of functionality may be dependent on third party resource providers who may need to be contacted directly for resolution.

III. PRICE AND PAYMENT

A. License fees have been agreed upon by EBSCO and the Licensee, and include all retrospective issues of the Product(s) as well as updates furnished during the term of this Agreement. The Licensee's obligations of payment shall be to EBSCO or its assignee. Payments are due upon receipt of invoice(s) and will be deemed delinquent if not received within thirty (30) days. Delinquent invoices are subject to interest charges of 12% per annum on the unpaid balance (or the maximum rate allowed by law if such rate is less than 12%). The Licensee will be liable for all costs of collection. Failure or delay in rendering payments due EBSCO under this Agreement will, at EBSCO's option, constitute material breach of this Agreement. If changes are made resulting in amendments to the listing of authorized Sites, Databases, Services and pricing identified in this Agreement, pro rata adjustments of the contracted price will be calculated by EBSCO and invoiced to the Licensee and/or Sites accordingly as of the date of any such changes. Payment will be due upon receipt of any additional pro rata invoices and will be deemed delinquent if not received within thirty (30) days of the invoice dates.

B. Taxes, if any, are not included in the agreed upon price and may be invoiced separately. Any taxes applicable to the Database(s) under this Agreement, whether or not such taxes are invoiced by EBSCO, will be the exclusive responsibility of the Licensee and/or Sites.

IV. TERMINATION

A. In the event of a breach of any of its obligations under this Agreement, Licensee shall have the right to remedy the breach within thirty (30) days upon receipt of written notice from EBSCO. Within the period of such notice, Licensee shall make every reasonable effort and document said effort to remedy such a breach and shall institute any reasonable procedures to prevent future occurrences of such breaches. If the Licensee fails to remedy such a breach within the period of thirty (30) days, EBSCO may (at its option) terminate this Agreement upon written notice to the Licensee.

B. If EBSCO becomes aware of a material breach of Licensee's obligations under this Agreement or a breach by Licensee or Authorized Users of the rights of EBSCO or its licensors or an infringement on the rights of EBSCO or its licensors, then EBSCO will notify the Licensee immediately in writing and shall have the right to temporarily suspend the Licensee's access to the Databases or Services. Licensee shall be given the opportunity to remedy the breach or infringement within thirty (30) days following receipt of written notice from EBSCO. Once the breach or infringement has been remedied or the offending activity halted, EBSCO shall reinstate access to the Databases or Services. If the Licensee does not satisfactorily remedy the offending activity within thirty (30) days, EBSCO may terminate this Agreement upon written notice to the Licensee.

C. The provisions set forth in Sections I, II and V of this Agreement shall survive the term of this Agreement and shall continue in force into perpetuity.

V. NOTICES OF CLAIMED COPYRIGHT INFRINGEMENT

EBSCO has appointed an agent to receive notifications of claims of copyright infringement regarding materials available or accessible on, through, or in connection with our services. Any person authorized to act for a copyright owner may notify us of such claims by contacting the following agent: Kim Stam, EBSCO Publishing, 10 Estes Street, Ipswich, MA 01938; phone: 978-356-6500, fax: 978-356-5191; email: kstam@ebsco.com. In contacting this agent, the contacting person must provide all relevant information, including the elements of notification set forth in 17 U.S.C. 512.

VI. GENERAL

A. Neither EBSCO nor its licensors will be liable or deemed to be in default for any delays or failure in performance resulting directly or indirectly from any cause or circumstance beyond its reasonable control, including but not limited to acts of God, war, riot, embargoes, acts of civil or military authority, rain, fire, flood, accidents, earthquake(s), strikes or labor shortages, transportation facilities shortages or failures of equipment, or failures of the Internet.

B. This Agreement and the license granted herein may not be assigned by the Licensee to any third party without written consent of EBSCO.

C. If any term or condition of this Agreement is found by a court of competent jurisdiction or administrative agency to be invalid or unenforceable, the remaining terms and conditions thereof shall remain in full force and effect so long as a valid Agreement is in effect.

D. If the Licensee and/or Sites use purchase orders in conjunction with this Agreement, then the Licensee and/or Sites agree that the following statement is hereby automatically made part of such purchase orders: "The terms and conditions set forth in the EBSCO License Agreement are made part of this purchase order and are in lieu of all terms and conditions, express or implied, in this purchase order, including any renewals hereof."

E. This Agreement and our Privacy Policy represent the entire agreement and understanding of the parties with respect to the subject matter hereof and supersede any and all prior agreements and understandings, written and/or oral. There are no representations, warranties, promises, covenants or undertakings, except as described in this Agreement and our Privacy Policy.

F. EBSCO grants to the Licensee a non-transferable right to utilize any IP addresses provided by EBSCO to Licensee to be used with the Services. EBSCO does not transfer any ownership of the IP addresses it provides to Licensee. In the event of termination of the Licensee's license to the Services, the Licensee's right to utilize such IP addresses will cease.

G. All information that EBSCO collects when Licensee accesses, uses, or provides access to, the Databases and Services is subject to EBSCO's Privacy Policy, which is incorporated herein by reference. By accessing or using the Databases and/or Services, you consent to all actions taken by EBSCO with respect to your information in compliance with the Privacy Policy.

DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "**Addendum**") is made effective on May 25, 2018 (the "**Addendum Effective Date**") by and between EBSCO Publishing, Inc. ("**Service Provider**") and Data Controller ("**Customer**"). This Addendum is being entered into in connection with and subject to the terms and conditions contained in the License Agreement between Service Provider and Customer (the "**Agreement**"). All capitalized terms used herein that are not otherwise defined shall have the same meaning as ascribed to such terms in the Agreement.

1. **Definitions**

a. "**Data Protection Legislation**" means the General Data Protection Regulation 2016/679 (GDPR) and any legislation and/or regulation implementing or made pursuant to the GDPR, or which amends, replaces, re-enacts or consolidates the GDPR.

b. "**data processor**", "**data controller**", "**data subject**", "**personal data**", "**processing**" and "**appropriate technical and organisational measures**" shall be interpreted in accordance with applicable Data Protection Legislation; and

c. "**Services**" shall have the meaning set forth in the Agreement (as applicable).

2. **Data Protection**

a. The provisions of this Section 1 shall apply to the personal data the Service Provider processes in the course of providing Customer the Services. Service Provider is the data processor in relation to the personal data that it processes in the course of providing Services to Customer. Customer is the data controller in relation to the personal data that it processed by data processor on its behalf in the course of providing Services to Customer.

b. The subject matter of the data processing is providing the Services and the processing will be carried out until Service Provider ceases to provide any Services to Customer. Annex 1 of this Addendum sets out the nature and purpose of the processing, the types of personal data Service Provider processes and the data subjects whose personal data is processed.

c. When the Service Provider processes personal data in the course of providing Services to you, Service Provider will:

i. process the personal data only in accordance with documented instructions from Customer (as set forth in this Addendum or the Agreement or as directed by Customer). If applicable law requires us to process the personal data for any other purpose, Service Provider will inform Customer of this requirement first, unless such law(s) prohibit this;

ii. notify Customer promptly if, in Service Provider's opinion, an instruction for the processing of personal data given by Customer infringes applicable Data Protection Legislation;

iii. assist Customer, taking into account the nature of the processing:

1. by appropriate technical and organizational measures and where possible, in fulfilling Customer's obligations to respond to requests from data subjects exercising their rights;

2. in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation, taking into account the information available to Service Provider; and

3. by making available to Customer all information reasonably requested by Customer for the purpose of demonstrating that Customer's obligations relating to

the appointment of processors as set out in Article 28 of the General Data Protection Regulation have been met.

iv. implement and maintain appropriate technical and organizational measures to protect the personal data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of personal data and appropriate to the nature of the personal data which is to be protected;

v. not give access to or transfer any personal data to any third party for such third party's independent use (e.g., not directly related to providing the Services) without Customer's prior written consent. If Service Provider provides personal data to third party subprocessors involved in providing the Service, Service Provider will include in our agreement with any such third party subprocessor terms which are at least as favorable to you as those contained herein and as are required by applicable Data Protection Legislation;

vi. ensure that Service Provider personnel required to access the personal data are subject to a binding duty of confidentiality with regard to such personal data;

vii. except as set forth in Section C.5 above or in accordance with documented instructions from Customer (as set forth in this Addendum or the Agreement or as directed by Customer), ensure that none of Service Provider personnel publish, disclose or divulge any personal data to any third party;

viii. upon expiration or earlier termination of the Agreement, upon Customer's written request, securely destroy or return to you such personal data, and destroy existing copies unless applicable laws require storage of such personal data; and

ix. at Service Provider's option, allow Customer and Customer's authorized representatives to either (i) access and review up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, data protection auditors) or suitable certifications to ensure compliance with the terms of this Addendum; or (ii) conduct audits or inspections, upon the parties mutual agreement, during the term of the Agreement to ensure compliance with the terms of this Addendum in accordance with this Section C.9. Notwithstanding the foregoing, any audit must be conducted during Service Provider's regular business hours, with reasonable advance notice to Service Provider and subject to reasonable confidentiality procedures. In addition, audits shall be limited to once per year, unless (a) Service Provider has experienced a Security Breach, as defined herein, within the prior twelve (12) months; or (b) an audit reveals a material noncompliance.

d. If Service Provider becomes aware of and confirms any accidental, unauthorized or unlawful destruction, loss, alteration, or disclosure of, or access to Customer's personal data that it processes in the course of providing the Services (a "**Security Breach**"), Service Provider will notify Customer within forty-eight hours.

e. All personal data processing is also covered by Service Provider's Privacy Shield certification. Service Provider agrees to (i) maintain Service Provider's Privacy Shield certification throughout the term of the Agreement, provided Privacy Shield certification remains a valid basis under the Data

Protection Legislation for establishing adequate protections in respect of a transfer of personal data outside of the European Economic Area or (ii) execute Standard Contractual Clauses in respect of the processing of such personal data. Service Provider will promptly notify Customer if Service Provider ceases to maintain, or anticipates the revocation or withdrawal, or are otherwise challenged by any regulatory authority as to the status of Service Provider's Privacy Shield certification, or if Service Provider makes a determination that it can no longer meet our obligations under Privacy Shield.

f. Prior to Service Provider processing personal data to Customer and Customer's users, Customer agrees to obtain a legal basis, which may include consent, for the processing of personal data in connection with the provisioning and use of Services. This Section (f) shall be in accordance with Article 6 of the GDPR or other applicable Data Protection Legislation.

3. MISCELLANEOUS

In the event of any conflict or inconsistency between the provisions of the Agreement and this Addendum, the provisions of this Addendum shall prevail. For avoidance of doubt and to the extent allowed by applicable law, any and all liability under this Addendum will be governed by the relevant provisions of the Agreement, including limitations of liability. Save as specifically modified and amended in this Addendum, all of the terms, provisions and requirements contained in the Agreement shall remain in full force and effect and govern this Addendum. Except as otherwise expressly provided herein, no supplement, modification, or amendment of this Addendum will be binding, unless executed in writing by a duly authorized representative of each party to this Addendum. If any provision of the Addendum is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of this Addendum shall remain operative and binding on the parties.

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

Subject to Agreement, Service Provider will provide the Services for the duration of the Agreement, unless otherwise agreed upon in writing.

The nature and purpose of the Processing of Company Personal Data

Service Provider will process all personal data governed by this Addendum as necessary to perform the Services pursuant to the Agreement, and as may be further instructed by Customer in its use of the Services.

The types of Company Personal Data to be Processed

Where applicable, as users are voluntarily permitted, but not required, may create a personalized account. Those accounts may collect the following limited personal data:

1. Name;
2. Email Address;
3. Password (in some cases); and
4. Security questions with answers.

The categories of Data Subjects to whom the Company Personal Data relates

Data subjects include Customer's current end-users.

ANNEX 2: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

Description of the technical and organizational security measures implemented by the Service Provider in accordance with the Addendum:

See attached Security White Paper.

White Paper: Information Security Practices

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 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,
Director, Information Security