ELSEVIER

Your Peace of Mind Is Our Priority

Our customers place their trust in us. It's a responsibility we take very seriously at Elsevier with a strong focus on data protection and security. We have instituted a variety of measures to maintain the security, integrity and availability of our products.

1. Dedicated Information Security Organization

Elsevier maintains a dedicated Information Security and Data Protection (ISDP) organization, headed by our Chief Information Security Officer (CISO). Elsevier security staff members have multiple years of experience in the industry and possess industry best practice certifications such as the Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Privacy Professional (CIPP), Certified Ethical Hacker (CEH) and multiple Global Information Assurance Certifications.

2. Risk–Mitigation Framework

Elsevier promotes the responsible use of information by employing a risk-management framework for information security based on the ISO 27002 framework. This framework includes administrative, physical and technical safeguards designed to reasonably protect the security of information collected from or about customers and end users.

3. Policies, Standards & Guidelines

Elsevier has implemented policies, standards and guidelines aligned with ISO 27002 domains that govern data access, protection, transport, restriction, retention, deletion and classification. Policies, standards and guidelines are reviewed and updated regularly.

4. Information Security Awareness Training

Elsevier employees receive regular data privacy and security awareness training. We equip employees with the knowledge to understand, identify and mitigate security risks by providing role-based secure application development training, phishing simulation tests and privacy and security campaigns.

5. Security Architecture & Design

Product environments are architected using industry-standard design principles and technologies. Elsevier products are deployed on enterprise class, highly available multi-tiered and segregated environments with security and access controls implemented at the network, systems and application layers.

Availability: Network and application designs utilize redundant systems, services and network connections. Servers are configured to be highly-available with redundant components such as power supplies and hard drives to provide uninterrupted service.

Business Continuity and Disaster Recovery: Service recovery plans are established to address potential service disrupting events. Application availability and system uptime are monitored constantly.

6. Vulnerability & Threat Management

Services, processes and technology are implemented to execute internal and external vulnerability scans to identify new application and system vulnerabilities. Identified risks are assessed for their potential impact along with determining appropriate response and remediation actions. We use a combination of network security testing, application security testing, application code review and penetration testing to assess our information security program and enhance it appropriately.

7. Application Security

Application design and secure coding best practices are implemented through process, procedures and technology as part of a defined software development lifecycle. Compliance to these requirements is validated through a combination of automated and manual review processes.

Elsevier has implemented several automated and manual solutions, which inspect applications and identify vulnerabilities that are then remediated:

DAST: Elsevier utilizes a Dynamic Application Security Testing (DAST) service to actively scan and monitor for vulnerabilities on our strategic applications. Our DAST service uses a combination of manual and automated

tests to identify and verify potential vulnerabilities.

SAST: Elsevier also uses Static Application Security Testing (SAST) to provide static code analysis to find and flag potential vulnerabilities as part of the development lifecycle. With SAST, teams can eliminate vulnerabilities before an attacker even has a chance to see them.

Manual Testing: Elsevier performs internal manual penetration tests on applications to find and identify vulnerabilities internally before an attacker can exploit them externally.

8. Data Security

To achieve a consistently high standard for data security, Elsevier utilizes a defense in depth methodology. This consists of controls and processes designed to protect against unauthorized access and alteration of data:

Host Security: Servers are deployed with base-lined hardened system images with non-essential services disabled or removed. Processes and technology are utilized to ensure security patches are kept up-to-date. Administrative access to hosts are controlled through roles and groups permissions, and access is logged and restricted to secure protocols and sources.

Encryption: We use industry standard encryption technologies for sensitive data in transmission and at rest to protect our data and make it unreadable to unauthorized users.

Physical Security: Data is stored and processed at physically secure data centers protected by segregated electronic security zones. Approved alarm systems monitor mechanical, electrical and environmental equipment. Intrusion alarms, video surveillance and onsite security staff further protect the data centers from unauthorized access.

Network Security: Elsevier utilizes a variety of network security technologies and processes to identify, prevent and detect unwanted traffic. Packet filtering firewalls and other access control devices limit unauthorized access to network segments.

Log Management: Logs and log management tools are used to capture a variety of usage data, application and system logs including but not limited to aggregated and anonymous usage activity (such as search queries), server activity and registered user logins. Access to logs is restricted with logs being securely stored based on their data classification.

Identity & Access Management: Access to our subscription products is restricted to authorized users and customers. User accounts, passwords, roles, groups and content subscription licenses are used to support appropriate authorization and authentication. User credentials are securely stored and protected. Elsevier has established processes and procedures for the provisioning, removal and review of access to our systems and applications.

9. Third Parties (Vendors & Suppliers)

Third parties who process data on behalf of Elsevier do so only for the purposes for which they are contracted. Additionally, they must use appropriate technical and organizational security measures necessary to safeguard the data.

10. Audit

A robust and detailed audit program is in operation to review and test policies, standards, guidelines and controls to assess their effectiveness. This audit program is based on the SSAE 16 and includes in-house and third-party audits as well as independent assessments.

11. Security Incident Response

A well-established, mature Security Incident Response process is used where incidents occur. Incident Response processes are in place and executed for all security incidents. Processes have been established for reporting and addressing events that may impact any aspect of the business. Security incident disclosures are conducted in accordance with internal, corporate-wide policy and in compliance with all appropriate regulatory policies and statutory guidelines which are applicable. Customer disclosure of breach which pertain to the affected customer services or subscribed entitlements are performed as required under international law or regulatory mandate.

Elsevier is committed to maintaining customer and user confidence and trust in our data protection and security practices.

For further information, please contact the Elsevier Chief Information Security Officer at CISO@elsevier.com.