PATHWAY STUDIO WEB SECURITY OVERVIEW
Pathway Studio Web is a comprehensive collection of information with powerful security features to ensure that your research is safe and secure.
Security Overview of Pathway Studio Web
The security and integrity of information that transits the Pathway Studio interface and server are of critical importance for our customers. Elsevier is committed to providing strong, industry-standard security systems to ensure the availability, confidentiality, and integrity of data, including intellectual property and sensitive personal information. Well-established information security policies, processes, and standards are in place within Elsevier, with systems that are maintained at a secured site to ensure around-the-clock protection.

PATHWAY STUDIO ENVIRONMENT
Pathway Studio is hosted at the LexisNexis Computing Complex in Dayton, Ohio, one of the largest data centers of its kind in the United States. That leading-edge facility contains some of the most sophisticated servers, software, and telecommunications equipment in the world. Support is provided 24/7 year round, and covers everything from automatic system updates to routine and emergency maintenance. Access to the data centers is restricted to cleared individuals with an approved business need. Elsevier office locations, and specifically data centers within these locations, are built with physical security in place that may include roaming security guards.

PATHWAY STUDIO MONITORING AND SUPPORT
The data center is constantly monitored by a team of system specialists and sophisticated monitoring software on both hardware and application levels. In addition, the Pathway Studio system is continuously monitored and maintained by two designated Pathway Studio system administrators, one located in Rockville, MD, and another in Frankfurt, Germany, ensuring 24-hour application-specific support for this system.

ARCHITECTURE AND NETWORK SECURITY
To ensure comprehensive and effective network security, Elsevier employs a “defense in depth” approach. The use of packet filtering, firewalls, and control devices limit access to Elsevier’s e-products. Intrusion detection and prevention devices are employed to filter out specific types of unwanted traffic. The Elsevier network is monitored constantly by automated and manual means, with support provided around the clock, as described in the previous section.

Redundancy and fault tolerance are guiding principles in the Pathway Studio architecture. The Elsevier network design utilizes redundant components and connections to ensure high availability. Several independent internet service providers ensure continuous connectivity to the Lexis-Nexis operation. LexisNexis firewalls and load-balancers distribute incoming requests onto a cluster of Dell PowerEdge Linux servers that are connected to the LexisNexis SAN infrastructure. This high-speed functionality ensures high availability and fast data access.
ACCESS CONTROL

Pathway Studio supports two access methods: username/password, and sitewide IP authentication, depending on the terms of the client’s license agreement. Both authentication methods require the Elsevier license administrator to check the validity of customer and user data before creating usernames or accepting IP ranges. That extra layer of security over the two options for access ensures that safety does not take a back seat to quick user access.

The process for each method of authentication is detailed below.

**Username / Password Authentication**

Typically, users self-register through the standard Pathway Studio interface, but user accounts can also be created through the Pathway Studio administration interface by the license administrator. In either case, usernames are unique throughout the whole system. The administrator must identify the user’s access credentials and the password is then chosen by the user. The password should satisfy the following rules:

- Password must meet a minimum length criterion
- Password must contain a minimum number of non-letter (number or symbol) characters
- Password must not match any of several easily guessed values related to the user’s personal information.

Pathway Studio uses state-of-the-art algorithms and processes for password encryption. User passwords are not stored directly in the authentication database; instead, a digest value calculated from the password plus an undisclosed salt value is held. The digest method is widely considered in the information security industry to be irreversible. The login process calculates the equivalent digest from the submitted password and allows authentication only if the two match. The password submitted during login is then immediately discarded.

When the user accesses Pathway Studio, the application server intercepts the request and displays a login page. The user enters the username and password into the login page. If the username and password are those of a user who has a role that is allowed to access Pathway Studio, the starting screen (main page) is displayed. Only users with the correct role can access Pathway Studio; all others are blocked at application server level.

**IP authentication**

Companies or institutions that want unlimited site-wide access to Pathway Studio are required to provide a public IP address or IP range to Elsevier. This address or range is used by Pathway Studio to ensure that anonymous user access is restricted to that specific site or system IP range. When a user from a company or institution with site-wide access attempts to access Pathway Studio, the application server intercepts the request and immediately displays the main page without presenting a login dialog. Only users within the given range of IP addresses can access Pathway Studio; all others are blocked at application server level.
Secure sockets layer (SLL) protocol

All data exchanged between the Pathway Studio server and a user are enciphered and transmitted via SSL. The SSL protocol is an industry-standard method for protecting Web communications and ensuring secure client/server communications. Using the SSL protocol, an SSL-enabled server can authenticate itself to an SSL-enabled client and the client can authenticate itself to the server, thereby establishing an encrypted connection between both machines. This encrypted connection provides “channel security,” which has three basic properties:

• The channel is private: encryption is used for all messages after a simple “handshake” defines a secret key. The initial key exchange is protected by Public Key Encryption.

• The channel is authenticated: the server endpoint of the conversation is always authenticated.

• The channel is reliable: the message transport includes a message integrity check.

An SSL connection provides a high degree of confidentiality by requiring that all information sent between a client and a server is encrypted by the sending software and decrypted by the receiving software. Any tampering with data sent over an encrypted SSL connection is automatically detected by a mechanism that determines whether the data have been altered in transit. SSL connections for Pathway Studio are managed by Elsevier. SSL encryption is validated by the certification authority, Trustwave Holdings, Inc. Trustwave issues a digital certificate, or electronic credential, confirming that Elsevier is the owner of Pathway Studio connections and thus enabling secure communications between client and server. For more information on Trustwave digital certificates, refer to: https://www.trustwave.com/.

Logging

As a further means of security for licensed customers, several events are logged on the Pathway Studio server:

• Logins and logouts

• Number of actions per user ID

• Type of actions, such as relation search or expression analysis

• Type of analyses performed, such as GSEA or SNEA

• Types of objects involved in actions and analyses.

Pathway Studio only logs the types of analyses conducted, but it does not log the actual data involved in the analysis. Elsevier is legally obligated to treat all stored data as confidential, and accordingly all license agreements entered into with customers reflect this fact.

Storing data

Pathway Studio creates temporary result sets for users in the course of their usage of the program. All temporary result sets created during a session are only stored during the session and are automatically deleted after the session has been closed. Temporary result sets, and all explicitly saved result sets, are only available to the given user logged into the system.

Pathway Studio provides output and export services, which generate data files in various formats on the Pathway Studio server for downloading. Those downloadable files are available as long as the download dialog box is visible and the current session is active. Once the session is closed all download files are automatically deleted.

Files with experiments uploaded by users, as well as pathways, entity lists and analysis results created by user within Pathway Studio are stored in the Pathway Studio database in non-encrypted form.
Web server security
Elsevier requires all servers hosting Pathway Studio to be “hardened” prior to use. The hardening process requires disabling or removing unnecessary services, ensuring that all needed security patches are current, and that all security mechanisms are enabled. Additional software, such as anti-virus and host-based intrusion detection systems, is installed where appropriate. Elsevier has a defined process to monitor for new vulnerabilities, assess their risk, determine the appropriate response and ensure that remediation takes place.

Elsevier employee security
Elsevier conducts background investigations, subject to local legal restrictions, commensurate to the level of security required of the job applicant. It also conducts reference checks on all personnel as a part of due diligence in the employment process. All Elsevier personnel are required to sign confidentiality agreements as a condition of employment.

Compliance
Elsevier has proven internal procedures for security risk assessment and compliance with internal policy across our worldwide network. Elsevier is compliant with Sarbanes-Oxley, and is audited annually.

Information security methodology and governance
Elsevier employs well-established and robust processes supporting the creation, maintenance, and approval of security policies and standards. The organization takes a risk-based approach to security to ensure that effective controls are implemented in the appropriate places. Training and certification of employees in security disciplines are also priorities. Employees with direct responsibility for security at Elsevier hold certifications such as the (ISC)² CISSP or GIAC GSEC.

Pathway Studio privacy policy
Elsevier is committed to maintaining the confidence and trust of customers with respect to the information collected from them. Refer to the Pathway Studio privacy policy at www.pathwaystudio.com/privacy.html for a complete description of the information collected about customers, how this information is used and the options customers have about how this information is used.
Visit elsevier.com/products/solutions/pathway-studio or contact your nearest Elsevier office.

ASIA AND AUSTRALIA
Tel: + 65 6349 0222
Email: sginfo@elsevier.com

JAPAN
Tel: + 81 3 5561 5034
Email: jpinfo@elsevier.com

KOREA AND TAIWAN
Tel: +82 2 6714 3000
Email: krinfo.corp@elsevier.com

EUROPE, MIDDLE EAST AND AFRICA
Tel: +31 20 485 3767
Email: nlinfo@elsevier.com

NORTH AMERICA, CENTRAL AMERICA AND CANADA
Tel: +1 888 615 4500
Email: usinfo@elsevier.com

SOUTH AMERICA
Tel: +55 21 3970 9300
Email: brinfo@elsevier.com

PATHWAY STUDIO is a registered trademark of Elsevier Inc. Copyright © 2015 Elsevier B.V. All rights reserved.
May 2015