Beneficial Ownership

Data Security and Protection

At Wolters Kluwer we understand the importance of application security in protecting your core company and beneficial owner information for reporting to FinCEN.

Design for Security

Our "design-for-security" framework and approach are an integral parts of our product development lifecycle from initial conceptualize through deployment and maintenance. We seek to optimize the performance, scalability, and availability of our applications by employing a private cloud infrastructure built with redundant backup that is designed to withstand unplanned activity and maintain continuous operations. Our secure product lifecycle methodology helps safeguard our web applications from unauthorized access or other malicious activity.

As your beneficial ownership information reporting partner, we are committed to safeguarding your sensitive information required in reporting to FinCEN.

Learn more about how we can help you securely file your beneficial ownership information reports.

Wolters Kluwer

Secure data storage

All data `at rest` is encrypted and decrypted using 256-bit AES encryption with RSA 2048-bit keys, one of the strongest block ciphers available, and is FIPS 140-2 compliant. All communication to the storage resources happens on an internal network where communication is encrypted using the highest supported standard with TLS 1.2 using at least AES 128 bit Cipher suites at a minimum.

End-to-end encrypted communication

All communication is encrypted using TLS 1.3 or TLS 1.2 with at least an AES 128-bit cipher depending on the capabilities of the client web browsers accessing the system. All inbound traffic is protected with an advanced Web Application Firewall which will detect and prevent malicious activities including Denial of Service attempts.

Isolated data processing

All data is being processed on isolated systems which are continuously monitored with threat detections systems to prevent malicious activity and supply chain attacks.

OIDC user authentication

The identity provider solution used in our Beneficial Ownership platform is the OpenId Connect (OIDC) authentication protocol. All credentials that are stored have their sensitive information hashed using the PBKDF2 hashing algorithm with 27500 iterations. Certain identities will be passed in through OpenID connect identity brokering and will inherit the security settings from the source identity provider.

Cloud-based security monitoring

All elements of the solution are managed with a state of the art Cloud Security Platform which provides Security Posture Management, Workload Protection and Infrastructure Entitlement Management to continuously monitor, alert and resolve any potential security risk.

Learn more about how we can help you securely file your beneficial ownership information reports.

Wolters Kluwer