Wolters Kluwer

Tax & Accounting Canada

CCH iFirm®

Data centre details, disaster recovery processes and security measures

Wolters Kluwer recognizes that information security is a critical concern and has developed a series of processes, policies and controls designed to provide for the confidentiality, integrity and availability of financial data for our CCH iFirm customers. This document provides an overview of Wolters Kluwer's efforts to employ a layered security model of threat remediation and defense for its CCH iFirm applications.

Wolters Kluwer will make every effort to accommodate requests for relevant data security information from our customers and prospects, as long as providing that information does not create a business risk.

***CCH iFirm* is hosted in a secure disaster-recovery configuration to protect our customers' data and to ensure continuous business operations using leading-edge technology**. Our hosted solution provides processing without burdening your firm with hardware costs, server management, hardware obsolescence, software updates, security and data centre operations staff. **Wolters Kluwer maintains two geographically diverse Canadian data centres in which hosting services for CCH iFirm are provided.**

Role and Need-Based Access
At Wolters Kluwer, team members only have the access they need, and that access is restricted to the discipline required of their current role. As team members change roles, gain new responsibilities or rotate on and off special projects, their access to systems and data is adjusted accordingly.

Maintenance
Procedures have been established to maintain system patch levels. Microsoft® products are used to develop a significant portion of the applications. We have established a process for testing security patches and service packs prior to installation in the hosted environment.

The criticality of the security patch is reviewed by IT Operations staff and deployed to a test environment for signoff by deployment and QA managers before production deployment application releases are evaluated and implemented on a scheduled basis.

Malware and Virus Scans
Each server is protected and governed by a malware and virus protection policy. The malware and virus protection engines are integrated with the infrastructure monitoring system. Virus definition DAT files are updated with real-time scanners enabled for all file I/O. Scheduled scans are also executed on devices. Virus alerts are monitored by support staff for remediation.

Data Centres and Redundant Systems
Wolters Kluwer uses SSAE 16, SOC 2, ISO 27002 and ISO 27018 certified datacentres. Each data centre solution includes redundancies to support our customer-facing applications. Wolters Kluwer data centres are currently required to meet Tier 3+ data centre specifications with redundant environmental controls, multiple ISP data paths, redundant electrical grid coverage and redundant generator/UPS systems on-site for emergency failover.

High Availability
Wolters Kluwer has invested in an active-active environment for CCH iFirm—designed to support the performance and availability of the service. This includes two separate production environments. Each environment is designed to achieve processing requirements at the peak load of tax season. In the event of some component or system failure, transactions are redirected to one environment until the incident is resolved.

Monitoring, Alerting and Incident Management
Wolters Kluwer utilizes an integrated monitoring, alerting and incident management system. We monitor utilizing synthetic transactions to verify actual application availability and performance from the customer's perspective. When any monitor triggers an alert, designated team members are alerted immediately via a paging system.

System Status
Our teams work hard to ensure that CCH iFirm is available 24/7. We provide customers with access to a product status page that can be consulted at any time to monitor the health of the application.

Backup Process
Controls are in place to provide for effective backups. Backups are encrypted. Copies of the backups are kept in a secondary location.

Active Penetration Testing
Wolters Kluwer subscribes to an independent service for external penetration testing. A report is provided to our IT team after each scan and any vulnerabilities discovered are assessed through change management.

Intrusion Detection
Automated intrusion detection systems detect and block unauthorized network activity.

Physical Security
Our service providers have deployed security measures designed to protect our physical assets from tampering, theft and destruction. This includes control access points, two-factor authentication with biometrics, security guards on-site, video cameras, etc.

Encryption
CCH iFirm encrypts all client/server communication via HTTPS Transport Layer Security protocols utilizing a SHA256 signed 2,048-bit certificate. Within CCH iFirm, data at rest is protected and stored in encrypted volumes via the AES 256-bit AES encryption, one of the strongest block ciphers available.

Multi-Factor Authentication (MFA)
All CCH iFirm users need to login to CCH iFirm using the Multi-Factor Authentication (MFA) process. This security measure is mandatory for all users. Note that this has also been implemented for users logging in to CCH iFirm Portal.

Information Security Policy
Wolters Kluwer has implemented a Global Information Security Policy that encompasses a variety of policies for managing information and technology assets based on data classification types intended to protect underlying applications and data exposure.

The Wolters Kluwer Global Information Security Policy dictates that each employee receives regular security awareness training on these policies and strictly prohibits the unauthorized viewing, use, duplication, destruction, transmission or modification of specific data types.

Continuous Improvement
Wolters Kluwer strives to meet a cyclic process of continuous improvement. Our IT teams meet regularly to discuss what worked, what may not have worked, and what changes are needed for improvement. This practice is designed to translate into fast and continuously improving service to our customers.

System and Organization Control (SOC) 2® Type 2 Compliance

Customer Benefits
CCH iFirm is subject to the rigorous demands of SOC 2® Type 2 audit and attestation because it provides confirmation for our customers of the implemented security measures to help in preventing breaches and securing their data. Furthermore, the SOC 2® Type 2 report informs our customers that CCH iFirm has met certain security criteria established to protect against unauthorized access (both physical and logical).

Scope
Wolters Kluwer has designed and implemented a control framework for CCH iFirm that is subject to annual examination by an external auditor and whose role is to express an opinion on the system description and on the suitability of design and operating effectiveness of controls stated in this system description.

Should you wish to receive CCH iFirm Canada SOC 2® report, please contact your sales consultant.

02/23 2023-M1599

Learn more. Contact your Wolters Kluwer sales consultant at 1 800 268 4522 or visit **www.wolterskluwer.ca** →

Wolters Kluwer