Wolters Kluwer

When you have to be right

Tax & Accounting

Information Security Measures for CCH Axcess™

Information security is a critical success factor for any person or service provider utilizing personal data of any kind — and for any reason. Wolters Kluwer recognizes the criticality of information security 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 Axcess customers. This white paper is intended to provide an overview of Wolters Kluwer's efforts to encompass a layered security model of threat remediation and defense for its CCH Axcess products.

CCH Axcess employs controls designed to provide for secure systems. To validate and attest to these controls, CCH Axcess has obtained AICPA industry-recognized Service Organization Controls Reports with attestation of controls. Currently SSAE16 and SOC2 Type II reports have been obtained for CCH Axcess. These reports are updated annually.

Wolters Kluwer will make every effort to accommodate any request for applicable data security information from our customers and prospects within our capabilities, so long as it is not a business risk. Please note however, that some information and items, such as SOC2 Type II reports, cannot be obtained without being a customer first.

Trust Services Principles and Criteria

Wolters Kluwer has developed a system of internal processes and controls for CCH Axcess based on the AICPA framework known as the Trust Services Principles and Criteria. We have developed processes and controls designed to protect our customers' interests with regard to service delivery, security and data protection. Our controls are reviewed annually by a certified external audit firm for effectiveness and relevance, and we follow AICPA SSAE16 Service Organizational Controls Reports and SOC2 principles and criteria.

Role and Need-Based Access

At Wolters Kluwer, each team member only has 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. Access is reviewed on set intervals to validate compliance with current job functions.

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.

CCH Axcess teams adhere to change management processes for all releases. A change request ticket is opened by the deployment team and is used to document and track the installation of software, patches and service packs and other maintenance performed in the hosted environment. An automated software deployment application is used to install patches as well as software in the application environment. All changes are evaluated using a risk calculation process. Changes considered high-risk or out of standard require appropriate evaluation for approval.

Release Management Process

Wolters Kluwer has developed an automated release management process and policy. A deployment process is rehearsed and supervised, and a log of all activities is created for each touch point during every release.

There are three types of releases that can occur:

- **Scheduled releases** occur based on a published schedule and generally happen at the same time each year. Depending on the time of the year, these releases may be weekly, monthly or there may be several months between releases.
- **Optional releases** are not on a published schedule but are made based on the availability of updated content needed by clients for compliance reasons. To allow for adequate testing prior to the release, an optional update requires at least 48 hours' notice when requested by any group. If the intent is to release an update with less than 48 hours' notice, it would be considered a critical release.
- **Critical releases** meet a critical security or client need and receive focused testing. Wolters Kluwer has implemented structured procedures designed to prevent excessive or unnecessary critical releases as they typically require action in less time than the 48 hour window that is afforded to optional releases.

If scheduled or optional releases are to be installed in the production environment, they will be performed within the following maintenance windows to minimize disruption to our clients.

- **Wednesdays** Midnight to 4 a.m. Central Time
- **Fridays** Midnight to 4 a.m. Central Time
- **Weekends** 10 p.m. Central Time (Saturday) to 6 a.m. Central Time (Sunday)

Change Management Process
Wolters Kluwer and our service providers have implemented a change management process. Change control review boards meet to review proposed changes for necessity, impact and risk — focusing on each change being appropriate and implemented correctly.

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 Centers and Redundant Systems
Each data center solution includes redundancies to support our customer-facing applications. Wolters Kluwer data centers are currently required to meet Tier 3+ data center 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 Axcess — 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. During normal operations, transactions are balanced between both environments, and 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. When any monitor triggers an alert, an incident management ticket is automatically opened and the designated team member is paged. Some monitors will automatically remove resources from service in the event of a serious malfunction.

Backup Process
We also have a backup process in place, including off-site media storage. Controls are in place to provide for effective backups. Backup tapes are encrypted. Copies of the backups are sent to off-site storage locations.

Quarterly Security Reviews
Each quarter, the IT teams review artifacts designed to measure whether our security controls and processes are working correctly. Vulnerabilities and account access are reviewed and logs are monitored as policy dictates.

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
Wolters Kluwer utilizes active intrusion detection systems capable of automatic threat remediation. The intrusion detection system is also integrated with monitoring systems that will generate alerts to team members and security staff as threats are detected.

Physical Security
Our service providers have deployed security measures designed to protect our physical assets from tampering, theft and destruction. This includes CCTV, security guards on-site, single entry no tailgating doors and RFID technology tracking.

Encryption
CCH Axcess encrypts all client/server communication via HTTPS Transport Layer Security (TLS 1.2) protocols utilizing a SHA256 signed 2048 bit certificate. Within CCH Axcess, data at rest is protected and stored in encrypted volumes via the AES 256 bit cipher via the Microsoft® Cryptography API at the application level.

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.

External Security Audits
Annually, Wolters Kluwer engages an outside third party auditing firm to review and align our processes and controls for CCH Axcess with current AICPA SOC standards and controls. Currently, Wolters Kluwer is utilizing SSAE16 and SOC2 Type II — which is equivalent to the AT101 and available for current CCH Axcess customers at the Customer Support site once they verify their account number and accept the terms for non-distribution.

Wolters Kluwer has and will continue to engage a third party to audit the effectiveness of our processes and controls.

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.

Contact information:
Wolters Kluwer
2700 Lake Cook Road
Riverwoods, IL 60015
United States
800-739-9998

Please visit **CCHGroup.com/Axcess** for more information.

1/17 2016-2375

Wolters Kluwer

When you have to be right