ENDNOTE ONLINE

SECURITY OVERVIEW FOR **MY.ENDNOTE.COM**

In line with commercial industry standards, Thomson Reuters employs a dedicated security team to protect our servers from attacks and other attempts to compromise the security and/or proper functioning of our IT and communications systems. These measures include deploying multiple firewalls and implementing proactive security scans and updates to prevent attacks on our systems and keep your data secure.

THOMSON REUTERS™

Document Version: X7
Date of Issue: May 2013

CONTENTS

GENERAL SECURITY

Thomson Reuters' global Information Security Risk Management (ISRM) team is responsible for ensuring that all Thomson Reuters' applications, platforms, and infrastructures are fully protected, and that our customer data is safeguarded at all time. The ISRM team certifies that on-going and regular audits, as well as security reviews against all Thomson Reuters applications, platforms, and infrastructures are conducted regularly. ISRM team members ensure that security posture of both infrastructure and application is improved by delivering security architecture designs, standards, and integrations across the entire Thomson Reuters global landscape. The ISRM security compliance team performs audit reviews in the areas of PCI, SOX, and other regulatory reviews to ensure that Thomson Reuters meets industry regulation requirements.

Thomson Reuters conducts both application and infrastructure vulnerability assessments regularly to ensure that the entire platform and application vulnerabilities are identified, reviewed, and mitigated. The Thomson Reuters Information Security policy is approved and sponsored by the Executive Committee. All Information Security Policies are reviewed and updated at a minimum of once per year. Thomson Reuters' asset management program is based on Information Technology Infrastructure Library (ITIL) disciplines and is subject to our ISO 27001 certification.

PHYSICAL SECURITY

All Thomson Reuters Facilities are secured by locked, electronically monitored doors. In addition, security guards monitor all entrances and require badges to enter. Visitors are required to be signed in and escorted, as well as have the appropriate badges. Multi-level security access is required for access to restricted areas. All access traffic is recorded, documented, and monitored across our Data Centers. Other security controls are implemented across Thomson Reuters to ensure full physical security protection of the Data Centers and their assets. Access to delivery and loading areas is controlled and monitored and deliveries and access are only allowed in controlled areas.

All employees are required to complete awareness training on the Company's Code of Business Conduct and Ethics that includes Information Security training. A company wide Global Role Framework exists that details roles and responsibilities, including security responsibilities. Further specialized training is completed based on job role, such as Application Developers and Customer Facing staff.

NETWORK AND HOST SECURITY

A number of standard security devices and solutions are in place to protect and safeguard both applications and data, and together make up the holistic enterprise security architecture and Data Center security strategy. The holistic prevention and protection strategies in place include firewalls, load balancers, log management, detection sensors, and vulnerability scanners. Also included are complete enterprise end-point solution tools like Anti-Virus, Anti-Spyware, Anti-Malware, and next generation intelligent security tools. Our report servers use Trend Micro.

Thomson Reuters' Security Operation Center (SOC) team provides on going security infrastructure and application monitoring. The SOC team utilizes advanced and next generation security tools and services to provide holistic security monitoring and protection to Thomson Reuter's assets around the globe. Detection and sensors, vulnerability scanners, and application white-listing tools are deployed across Data Centers to monitor and / or block malicious activities including spoofing, hijacking, and DOS. Other security tools, including protection tools, are in place to protect Thomson Reuters' on-demand and internal applications and platforms. Thomson Reuters has Intrusion Detection Systems (IDS) and other proactive security monitoring tools in place to ensure that the Data Centers are monitored around the clock. Further, a dedicated team of security analysts provide continuous monitoring and analysis of the latest security threats, to ensure malicious activities are identified and defeated immediately.

Thomson Reuters' ISRM team provides security risk assessments, application and infrastructure vulnerability assessment through the Enterprise Security Services (ESS) group, who in turn conduct regular threat and vulnerability assessments against Thomson Reuters platforms and applications. The ISRM team also provides Application Security Assessments (ASAs) against Thomson Reuters applications to ensure security controls are integrated and implemented. Any critical code flaws are identified and fixed by the development community of Thomson Reuters. Further, the ESS group also works with industry leading security groups to conduct 3rd party security reviews against Thomson Reuters applications and platforms.

As part of Thomson Reuters Multi-Layer Security (MLS) architecture, enterprise version firewalls by both Cisco and Juniper are implemented across different zones to secure and protect applications. All firewall devices follow the Thomson Reuters SLA to receive the latest vendor updates and patches. Firewall logs are collected in addition to other Data Center network device logs, and all logs are analysed by the SOC team. Additional network security tools are in place to monitor security activities across the entire infrastructure.

ONLINE SECURITY

EndNote online (my.endnote.com) offers Secure Sockets Layer (SSL) connections for subscribers. The SSL security protocol provides an https secured connection that supports 128-bit encryption of the following requests to the ***my.endnote.com*** site: Registration, Log-in, Format Paper, Sync Services, Authentication for Transfer, and Authentication for **Cite While You Write**™ (CWYW). This is the same technology that most e-commerce websites use to encrypt credit card information and is the industry standard security protocol for protecting sensitive data while in transit.

my.endnote.com offers browser and Word plugins. The CWYW plugin for Word is optional, but is needed in order to have integration with Word for citations. The IE and Firefox browser plugin installers can be downloaded separately. All plugins use SSL for user authentication requests.

my.endnote.com log files are recorded on production in line with the requirements for incident investigation and event monitoring. Access to production systems is restricted to authorized users and production systems are housed in computer suites with controlled entry. Where logs are backed up to removable media, this media is handled and sent off-site according to local media handling procedures. Web Services are used to access internal content from ***Thomson Reuters Web of Knowledge***℠, whose servers are also located in Eagan, Minnesota, US.

If you are using the ***EndNote*** desktop client in addition to ***my.endnote.com***, all communication between the desktop and online is encrypted (i.e., travels over SSL) when synchronizing ***EndNote*** X6 and X7 libraries. In ***EndNote*** X5 (and earlier) Transfer, only authentication calls to ***my.endnote.com*** are encrypted, and all other communication is unencrypted.

THOMSON REUTERS™

DISASTER RECOVERY

Our business continuity strategy for the ***EndNote online (my.endnote.com)*** application and services includes redundant servers, network components, and storage systems for High Availability (HA) capability on products and components. While we have redundant servers, there is no Data Center redundancy currently in place.

There is no routinely scheduled downtime for ***EndNote online (my.endnote.com)***, but in the case that it needs to be taken offline for maintenance and fixes, a flash message is posted on the product 48–72 hours prior to a scheduled or planned update/patch. As far as backup and recovery for the ***EndNote online (my.endnote.com)*** application and services, regular backups are done daily at a scheduled time for references. File attachments are not backed up, but make use of dual-framed redundant storage.

SUPPORT

my.endnote.com supports certifications and standards, and provides a VPAT document for each release. You can access the information for the current version at http://endnote.com/support/ada-compliance.

Our support policy always covers the latest three desktop releases. As of this document's issue date, these are X7, X6, and X5. This does not include compatibility support for new operating systems and word processors introduced after a release that are not covered by that version's system requirements.

EndNote includes a full Help system and Getting Started Guide installed with the application. We also provide free training videos and webinars detailed at http://www.endnote.com/training/.

Feel free to contact Customer Support at http://endnote.com/contact/customer-support.

For more information
Send us a sales enquiry at rs.sales@thomsonreuters.com
Read more about our products at endnote.com
Find out how to contact your local office
endnote.com/contact

Document Version : X7
Date of Issue : May 2013

THOMSON REUTERS™