ENDNOTE SECURITY OVERVIEW INCLUDING ENDNOTE DESKTOP AND ONLINE

INTRODUCTION

In line with commercial industry standards, the data center used by EndNote 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.

CONTENTS

GENERAL SECURITY

Clarivate Analytics Global Information Security Risk Management (ISRM) team is responsible for ensuring that all Clarivate Analytics applications, platforms, and infrastructures are fully protected, and that our customer data is safeguarded at all time. The ISRM team conducts that on-going and regular security audits, as well as security reviews against all Clarivate Analytics 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 Clarivate Analytics global landscape. The ISRM security compliance team performs audit reviews in the areas of PCI, SOX, and other regulatory reviews where required to ensure that Clarivate Analytics meets industry regulation requirements.

Clarivate Analytics conducts both application and infrastructure vulnerability assessments regularly to ensure that the entire platform and application vulnerabilities are identified, reviewed, and mitigated. The Clarivate Analytics 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. Clarivate Analytics asset management program is based on Information Technology Infrastructure Library (ITIL) disciplines and is subject to our ISO 27001 certification.

All Clarivate Analytics 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 Clarivate Analytics 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 companywide 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.

Clarivate Analytics 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 Clarivate Analytics 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 Clarivate Analytics on-demand and internal applications and platforms. Clarivate Analytics 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.

Clarivate Analytics 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 Clarivate Analytics platforms and applications. The ISRM team also provides Application Security Assessments (ASAs) against Clarivate Analytics applications to ensure security controls are integrated and implemented. Any critical code flaws are identified and fixed by the development community of Clarivate Analytics. Further, the ESS group also works with industry leading security groups to conduct 3rd party security reviews against Clarivate Analytics applications and platforms where required.

As part of Clarivate Analytics Multi-Layer Security (MLS) architecture, enterprise version firewalls by multiple world-class industry vendors are implemented across different zones to secure and protect applications. All firewall devices follow the Clarivate Analytics SLA to receive the latest vendor updates and patches. SOC will utilize network logs and other logs to assess and identify cyber threats. Additional network security tools are in place to monitor security activities across the entire infrastructure.

ONLINE SECURITY

EndNote online 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 ***EndNote online*** site: Registration, Log-in, Format Paper, Sync Services, 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.

EndNote online 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.

EndNote online 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 the ***Web of Science*** ™, whose servers are also located in Eagan, Minnesota, US.

If you are using the ***EndNote*** desktop client in addition to ***EndNote online,*** meaning you are Syncing and or Sharing you library, or having a library shared to you by another EndNote X7.2 or later user, all communication between the desktop and online is encrypted (i.e., travels over SSL) when synchronizing

EndNote X7 and later libraries. In ***EndNote*** X5 (and earlier) Transfer, only authentication calls to ***EndNote online*** are encrypted, and all other communication is unencrypted.

DISASTER RECOVERY

Our business continuity strategy for the ***EndNote online*** 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***, 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*** 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.

USE IN VIRTUAL ENVIRONMENTS

Does EndNote work with Citrix Application Hosting?

We do not officially support use in this environment and have documented additional details here: http://endnote.com/kb/82193

Does Endnote support use over Virtual Private Network (VPN)?

We do not officially support use in this environment. Libraries can be opened while on local storage or a fast LAN connection (e.g., same building). There are known performance issues trying to open a library from off-site locations that can lead to library corruption. Due to this potential risk, we do not recommend this particular use.

CUSTOMIZATION

What customizations are available?

EndNote allows the end user to customize:

- Bibliographic Styles
- Import Filters
- Connection Files
- Central location of styles, filters and connections for network environment
- Definition of reference types and fields
- OpenURL Links and Proxy URLs for Find Full Text
- Duplicate field control
- Spellcheck terms and language
- Term Lists for synonym control with Journal titles
- Display fonts and fields

These customizations are also available to the administrator for mass installation using the MSI.

COMMON PORTS USED FOR ONLINE SEARCH

210 is the base port used for most sites and thereby the *__most__* commonly used by Horizon and Innopac servers. 2100 is also commonly used by Innopac systems, 2200 is the default for Unicorn systems, and 7090 is common to the Voyager system, including the Library of Congress.

210, 2020, 2100, 2101, 2121, 2200, 3950, 5666, 7090, 7190, 7290, 7390, 7490, 7690, 7890, 9909, 9991, 9999, 20011, 20012, 21210

LESS COMMON PORTS USED FOR ONLINE SEARCH

211, 212, 220, 221, 223, 1111, 1616, 1921, 2010, 2102, 2103, 2104, 2108, 2111, 2112, 2113, 2116, 2132, 2203, 2205, 2210, 2211, 2222, 2227, 2300, 2400, 2500, 2600, 2800, 3200, 3333, 4151, 4201, 4210, 5009, 5200, 5205, 5210, 5302, 5305, 5405, 5500, 5505, 5605, 5705, 5805, 6005, 6105, 6205, 6305, 6333, 6405, 6433, 6505, 6605, 6705, 6805, 6905, 7005, 7019, 7025, 7091, 7099, 7105, 7205, 7280, 7305, 7405, 7505, 7590, 7605, 7705, 7788, 7790, 7805, 7819, 7990, 8010, 8019, 8090, 8105, 8110, 8190, 8205, 8305, 8888, 9190, 9290, 9390, 9490, 9535, 9590, 9690, 9825, 9830, 9840, 9850, 9855, 9860, 9865, 9870, 9875, 9880, 9885, 9895, 9929, 9949, 9992, 9993, 9996, 9997, 9998, 10090, 10190, 10290, 10390, 10490, 10646, 10790, 10890, 10990, 11090, 11390, 11490, 11590, 12090, 12490, 12590, 12690, 12890, 12990, 13090, 13190, 13290, 13390, 13490, 13590, 17590, 18290, 20010, 24210, 55200, 57090

SYSTEM REQUIREMENTS

What are the EndNote X8 System Requirements?

http://endnote.com/product-details/compatibility

SUPPORT

Our support policy covers EndNote desktop versions X7 and X8. 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.