REMOTE DEPOSITION | SECURITY GUIDE

Remote proceedings managed by Veritext provide the highest level of assurance that your clients' confidential information is protected and secure. Our system and operations comply with HIPAA (Health Insurance Portability and Accountability Act) security standards as a business associate and meet federal and state requirements for handling PII (Personally Identifiable Information).

At Veritext, we take information security seriously. As part of our Information Security Policy, Veritext undertakes a technology audit annually, regularly performs operational and systems risk and vulnerability assessments, performs annual risk assessments of 3rd party service and technology providers, and is currently in the process of undergoing a SOC-2 audit.

VERITEXT LEGAL SOLUTIONS

VERITEXT'S PLATFORM

Veritext Virtual 3 is built on the Zoom platform and offers a streamlined interface. Veritext Virtual 3 offers a flexible platform with many user-friendly features and exceptional handling of demanding presentation and video capture requirements as well as lower or less reliable network connectivity. The controls for Veritext Virtual 3.0 include capabilities for waiting rooms, private breakout rooms and more.

It is a proven, highly effective application which is rigorously managed and secure. The Veritext standard configuration settings allow for the strongest securities which, as aforementioned, comply with HIPAA as a business associate and PII security standards.

SECURITY CONFIGURATION

The fundamental security aspects of the Zoom platform is equivalent with other reputable commercially available conferencing platforms on the market today. The keys to ensuring information privacy and confidentiality on any web conferencing platform are:

- **Effective Identity and Authentication Management**
- **Appropriate Configuration Management**
- **Sound Support and Usage Practices**

Let's explore each of those aspects of securely managing these services . . .

IDENTIFICATION AND AUTHENTICATION MANAGEMENT

The majority of reported cybersecurity exploits on systems are based on compromises in identity and authentication. Web conferencing platforms are no exception.

The challenging factor in the web conferencing arena is the tendency to treat high-security applications such as legal proceedings in the same manner as a video conference with friends or intra-company business colleagues.

At Veritext, we provide unique user id and self-managed password credentials to all participants in the remote proceeding. This ensures that all participants are identified and authenticated at entry.

CONFIGURATION MANAGEMENT

As with Authentication Management, all major web conferencing platforms provide configuration options that, when appropriately applied, can provide a highly secure environment. Veritext manages each of its platforms so Vulnerabilities are mitigated by following configuration management points.

FILE SHARING DISABLED

Veritext configures its remote proceedings to turn off file sharing, which eliminates the potential for inappropriate or malicious content distribution. Files to be distributed as part of a legal proceeding are managed by the authorized host via the exhibit sharing tools provided for that purpose.

PRESENTATION MODE DISABLED FOR NON-HOSTS

Veritext configures its remote proceedings to lock out participants from presenting content unless explicitly permitted by the host during the meeting, which eliminates the potential for inappropriate or private content to be exposed.

ENCRYPTION OF CONTENT

Veritext remote proceedings are always configured to encrypt all content at the application layer using an Advanced Encryption Standard (AES) 256-bit algorithm. This mitigates any potential network vulnerability causing unauthorized data capture on the wire.

PERSONAL CHAT DISABLED

Veritext turns off private chat for our remote proceedings, which eliminates the potential for inappropriate or illicit back-channel communication.

SUPPORT AND USAGE

Information security on the most secure platforms is only as good as the practices applied in usage. Veritext provides the following support to ensure the most secure and effective usage of its platforms.

REPORTER AND VIDEO TECHNICIAN PROTOCOL

All Veritext independent contractor partners agree to follow Veritext's stringent information privacy and confidentiality policy. In addition, those providing their services using our remote platforms are briefed on support and client usage practices to assist in assuring best practices in conducting a confidential remote proceeding.

CLIENT AND PARTICIPANT REMOTE PRACTICE GUIDANCE

Veritext provides a Client Practice Guide to assist clients in conducting proceedings in an effective and secure manner. This mitigates the risk of inadvertent breach of confidential information due to missteps in utilizing controls or sharing content. See the practice guide here https://www.veritext.com/remote-practiceguide/.

Key practice considerations outlined are as follows:

Participant Waiting Room Usage: Remote proceedings can be configured to utilize "waiting rooms" where participants are unable to enter the conference until explicitly permitted by the host. This provides another layer, in addition to unique User ID and Password management, of protection against inappropriate or unauthorized entrants into the conference. This feature works for both video and telephone-only entrants.

Participant Blacklisting: Hosts are able to lock any participant from the meeting, and that participant will be unable to enter without explicit reapproval of the host.

Participant Admonishments: A set of recommended remote proceeding instructions are provided to ensure appropriate engagement and efficient communication and capture of the record.

TECHNICAL SUPPORT

Veritext provides pre-event setup support to ensure that all participants have valid credentials, appropriately supported devices and adequate connectivity as well as on-call technical support for all remote proceedings. Optionally, Veritext can serve as host support to provide "eyes and hands" for the noticing attorney to ensure that all controls and content presentation are effectively and securely executed.

A WORD ABOUT THE RECENT PRESS ON ZOOM

(MARCH-APRIL 2020)

Zoom has been the subject of press reports around unauthorized access and inappropriate content sharing labeled "Zoom-bombing," and certain technical aspects of their platform have been called into question. As noted herein, Veritext performs risk assessments of every one of our platform providers and has recently completed such an assessment of Zoom. That assessment concluded that, when configured and utilized appropriately, Zoom is a highly secure and effective platform and as secure as any other platform on the market.

While the Press reports on Zoom exploits are serious considerations, in all cases those exploits are in the context of consumer and general business communication where secure configuration and use practices are generally very lax. Veritext Virtual, and our setup and practices, utilize the Zoom platform in a way that completely mitigates such risks, many of which are present on any web conferencing platform on the market.

VERITEXT LEGAL SOLUTIONS

ZOOM PLATFORM RISK ASSESSMENT SUMMARY

SECURITY CERTIFICATIONS

Zoom maintains a current SOC-2 Type 2 attestation, a FedRAMP Authorization to Operate and an EU-US Privacy Shield certification, which are indicators of a very sound policy and controls environment.

IDENTIFICATION PROTOCOLS

Veritext Virtual identification and authentication, as noted herein, fully mitigates the risk around unauthorized entry that all Zoom-Bombing exploits utilized.

PRESENTATION AND FILE SHARING PROTOCOLS

Veritext Virtual participant presentation and file sharing lockdown fully mitigates the risk of unauthorized content presentation and communication found in Zoom-Bombing attacks.

WAITING ROOM PROTOCOLS

Enabling of waiting room and blacklisting options fully mitigate the risk of an unauthorized party accessing or presenting information due to a participant compromising their credentials.

ENCRYPTION ASSESSMENT

Reports criticizing Zoom's encryption algorithm TLS (256 AES bit encryption) do not present a credible or practical vulnerability and no reported exploits have been reported. The only exploits regarding unauthorized content access were in situations where encryption was not configured for the session, which any platform would suffer given the poor configuration choice.

NO VULNERABILITIES

As of this writing, there are no reported security vulnerabilities in any of the Zoom client software distributions.

ADDITIONAL INFORMATION:

VIEW THE ZOOM SECURITY LETTER FROM EXECUTIVES AND ARTICLE: Key Zoom Features for Secure Meetings

For additional information or questions about any of Veritext's security practices, please contact your Veritext account or client services representative.